NOAALINK EXAMPLE

U.S. Department of Commerce
NOAA
IT Service Support Performance Work Statement

1/1/2014
1.0 Detailed PWS Information

1.01 Background: The National Oceanic and Atmospheric Administration (NOAA), which plays several distinct roles within the Department of Commerce (DOC), is focused on the condition of the oceans and the atmosphere. NOAA is comprised of various Line, Staff, and Program Offices that serve as vital contributors to NOAA’s mission.

NOAA’s Information Technology organizations oversees activities in IT security, information systems operations, and information systems development and modernization. Specialized technical expertise to support these activities is required in security certification and accreditation and continuous monitoring of national critical information systems, earned value and portfolio analysis of complex programs, and engineering support for data networks and telecommunications that span across the enterprise.

Given the rapidly changing IT infrastructure and operations supported by NOAA, with the addition of program management and potential consolidation activities, it is critical that the senior management within this organization have access to the latest information on enterprise IT support and services.

NOAA also promotes and shapes an effective strategic and operational IT planning process, coordinates the preparation of IT budget and associated materials, oversees selected operational IT systems and services, and is responsible for other assigned programs.

1.02 Objectives: The overarching objectives of the support described in this PWS are to:

- Facilitate the development, deployment, operation and expansion of critical standard, services and infrastructure
- Document IT guidelines and technical standards to ensure ease of implementation by partners
- Ensure that technical projects are executed on schedule, within budget, and in accordance with technical requirements
- Assist in the planning for future services and infrastructure

1.03 Scope/High-level Description: This PWS describes the scope of work, objectives, tasks and resources needed to successfully fulfill NOAA’s IT support related responsibilities to advance the organization’s mission. As a result, NOAA must establish these capabilities in order to better collaborate with its business partners, prioritize IT projects, select high value opportunities to enhance services, and effectively and efficiently operate the organization’s IT resources. NOAA requires information technology services in enterprise architecture, strategic planning, technical operations and maintenance, portfolio management, cost reduction methodologies, business case analyses, and a variety of IT ad hoc requests.

- Systems engineering, software, and hardware
- Systems architecture, systems analysis, and systems design
- Multiple programming languages
- Computer hardware upgrades, i.e. servers, network components, desktops
- Multiple operating systems
- Implementation of a Service Oriented Architecture
- Engineering and/or scientific expertise

1.04 Requirements: The task requirements are:

- Software and systems support in analyzing, troubleshooting, testing and making recommendations related to systems environment
  - Work in coordination with other network efforts NOAA-wide to improve the network performance.
  - Implement all networking security standards to the networking equipment that resides on the network in accordance with security policies.
  - Provide central services for Windows based computers
- Provide Active Directory services to allow administrators to assign policies, deploy software, and apply critical updates to the LAN infrastructure.
- Maintain and troubleshoot all approved Internet and Internetwork connections to the operational and administrative networks within the systems.
- Maintain and troubleshoot all network software on the administrative network.
- Perform configuration, installation and other system administration functions as necessary
  - Manage the directory servers for the system administrative network domains. As requested by the organization, and approved by the administrative network System Managers, set up and maintain accounts and access groups as well as folder and file sharing capabilities.
  - Provide Operating System (OS) Services and Administration to include enterprise system management, server and SAN administrations, security boundary administration, file services, print services, DHCP, Window Internet Naming Services (WINS), management storage services, Windows systems administration and user account management.
  - Provides Windows Administration:
    - Provide central authentication and authorization services.
    - Analyze data stored on the Windows system and make recommendations relating to performance and efficiency of that data storage.
- Software engineering support in the integration of existing baseline and non-baseline software into the systems environment
  - Define and document customer needs and requirements and develop and establish system specifications
- Troubleshoot, diagnose, and resolve outages and other problems with web servers, data processing servers, and database servers
  - Provide for Incident Response and Problem Management including root cause of system problems, such as configuration issues resulting in operational performance degradation or system outages, supporting the local manager with information and advice on the necessary corrective actions and/or interim workarounds. The associated operational support process requires careful management and planning to ensure optimal results at all times. Incident Response activities include: problem identification, recording, classification, diagnosis, metrics, and reporting. Error Control includes providing correction of configuration items to resolve or remove errors, faults, or inconsistencies, in conjunction with the overall management of known errors while they remain unresolved and until they are eliminated by the successful implementation of changes made under the change control process. The Contractor will be responsible for the resolution of issues / trouble tickets in a timely manner and within the prescribed Service Level Agreements (SLAs) established by the appropriate organizations. IT Security requires reporting all possible incidents to the Security Officer or System Owner as appropriate on a case by case basis, and following their provided direction as well as established IT Security Incident policy. This includes providing required assistance and all required documentation for all IT security incidents.
- Ensure all systems are Federal Information Security Management Act (FISMA) compliant
- Serve as the third party security assessor for Security Authorization process and assist in preparing required documentation packages
- Support field System Administrators to maintain NOAA baseline security configurations on systems and check if all the security patches and service packs are appropriately installed on systems
- Perform system utilization analysis and feasibility studies for system upgrade projects
- Assist in preparing security plans, policies, guidelines, and standards for systems and system users in order to implement NOAA security directives and policies
  - The Contractor provides one or more ISSOs to assist the federal SO develop and maintain an IT security program that addresses implementation of Federal Information Security Management Act (FISMA) requirements as mandated by the White House Office of Management and Budget (OMB), in accordance with NIST Standards and special publications; and DOC and NOAA Security policies and procedures. The ISSO must meet the DOC CITR-006, Information System Security Training for Significant Roles, requirements for professional certification, and annual role-based training.
o The Contractor shall examine documentation and assist in implementing any new requirements promulgated by law and government policy
o Other security-related activities:
  ▪ Perform risk analyses
  ▪ Perform IT installation reviews and security
  ▪ The Contractor advises how to manage information-security related risks. More specifically, the Contractor helps implement controls to sustain and improve the confidentiality, integrity, and availability of the LAN data and its delivery systems. These goals are relevant whether the data are in storage, processing, or transit, and whether threatened by malice or accident.

1.05 Deliverables:

<table>
<thead>
<tr>
<th>Deliverable</th>
<th>Frequency</th>
<th>Medium/Format/# of Copies</th>
<th>Submit To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kick Off Meeting</td>
<td>Within 20 days of award</td>
<td>1</td>
<td>Consult with TM, COR, and CO to schedule</td>
</tr>
<tr>
<td>Project Management Plan</td>
<td>Within 30 days of award</td>
<td>1 copy submitted via email</td>
<td>TM, COR</td>
</tr>
<tr>
<td>Monthly Activity Report</td>
<td>By the 15th of every month</td>
<td>via email</td>
<td><a href="mailto:noaalink.invoice@noaa.gov">noaalink.invoice@noaa.gov</a></td>
</tr>
<tr>
<td>LOE Spend Plan</td>
<td>Within 10 days of award; ongoing updated on a monthly basis by the 15th of the month</td>
<td>via email using NOAALink instructions</td>
<td><a href="mailto:noaalink.invoice@noaa.gov">noaalink.invoice@noaa.gov</a></td>
</tr>
<tr>
<td>IT Guidelines and Technical Standards</td>
<td>As required</td>
<td>via email</td>
<td>TM, COR</td>
</tr>
<tr>
<td>Attendance and participation at Project Status Meeting</td>
<td>Weekly</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Attendance and participation at Task Planning Meeting</td>
<td>Weekly</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Update ticket information with technical status and actions taken</td>
<td>Daily or as appropriate</td>
<td>Electronic</td>
<td>Enter into ticket tracking tool</td>
</tr>
<tr>
<td>Update testing results document detailing testing of new release software</td>
<td>Each release</td>
<td>Electronic</td>
<td>Enter into release tracking tool</td>
</tr>
</tbody>
</table>
1.06 Constraints:
   1. Future budgets are unknown and may impact the successful continuation or completion of this statement of objectives.
   2. General government participation and involvement may be limited due to other competing corporate priorities.
   3. NOAA does not have a mature ITIL process. NOAA does not have a documented “as-is” or “to-be” enterprise architecture.

1.07 Period of Performance: The period of performance shall be for one (1) Base Year of 12 months and two (2) 12-month option years. The Period of Performance reads as follows:

   Base Year – September 24, 2012 to September 23, 2013
   Option Year I – September 24, 2013 to September 23, 2014
   Option Year II – September 24, 2014 to September 23, 2015

The Government reserves the right to extend the term of this contract at the prices set forth in Section B in accordance with the terms and conditions contained in clause 52.217-9 entitled, “Option to Extend the Term of the Contract”.

1.08 Type of Order: The government anticipates award of a Time and Materials (T&M) contract.

1.09 Hours of Operation/Place of Performance: The contractor is responsible for performing between the hours of 8:30 a.m. and 5:00 p.m. Monday through Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The contractor must at all times maintain an adequate work force for the uninterrupted performance of all tasks defined within this statement of work when the Government facility is not closed for the above reasons. When hiring personnel, the contractor shall keep in mind that the stability and continuity of the work force are essential.

Work will normally be performed at the National Oceanic and Atmospheric Administration, 1335 East West Highway, Silver Spring, MD 20910. Remote work is authorized and will be scheduled and monitored at the discretion of the TM and must comply with the Department of Commerce Information Technology Requirement (CITR) 0008: Remote Access.

Travel under this task award may be necessary in order to accomplish certain task(s) contained in this task award. Travel must be deemed necessary and authorized by the TM in order to be paid for by the Government. Except for exceptional circumstances, travel will not be reimbursed at more than applicable rates cited in the Federal Travel Regulations, prescribed by the General Services Administration, for travel in the conterminous 48 United States or the Standardized Regulations (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas," prescribed by the Department of State, for travel in areas not covered above.

1.010 Special Qualifications: The contractor IT operations staff must be Microsoft Certified Solutions Associate (MCSA) certified in server, database, and developer. The contractor IT security staff must be Certified Information Systems Security Professionals (CISSP). The contractor staff handling project management duties must be Project Management Professional (PMP) certified. The contractor is expected to provide a fully trained workforce to the government; therefore, personal development training costs and hours are not billable to the government.

1.011 Recognized Holidays:

   New Year’s Day             Labor Day
   Martin Luther King Jr.’s Birthday   Columbus Day
   President’s Day            Veteran’s Day
   Memorial Day               Thanksgiving Day
   Independence Day           Christmas Day
In addition to the days designated as holidays, the Government observes the following days:
Any other day designated by Federal Statute
Any other day designated by Executive Order
Any other day designated by a President's Proclamation

It is understood and agreed between the Government and the contractor that observance of such days by Government personnel shall not otherwise be a reason for an additional period of performance, or entitlement to compensation except as set forth within the contract. If a contractor believes that an unplanned absence has an impact on the price or period of performance, it should notify the contracting officer (CO) of the changed condition and submit a claim for equitable adjustment (see FAR 52.233-1).

Nothing in this clause abrogates the rights and responsibilities of the parties relating to "stop work" provisions as cited in other sections of this contract.

1.012 Security Requirements:

1.0120 The systems supported under this task are High security.

1.0121 Suitability/Risk Level - The suitability or risk level for this work has been determined to be: High. As such, the contractor shall pre-screen their employees to eliminate anyone who does not meet the following criteria: The prospective employees must be U.S. Citizens and Foreign Nationals.

48 CFR 1352.237-70 - Security Processing Requirements—High or Moderate Risk Contracts (APR 2010)
(a) Investigative Requirements for High and Moderate Risk Contracts. All contractor (and subcontractor) personnel proposed to be employed under a High or Moderate Risk contract shall undergo security processing by the Department's Office of Security before being eligible to work on the premises of any Department of Commerce owned, leased, or controlled facility in the United States or overseas, or to obtain access to a Department of Commerce IT system. All Department of Commerce security processing pertinent to this contract will be conducted at no cost to the contractor. The level of contract risk will determine the type and scope of such processing, as noted below.
(1) Investigative requirements for Non-IT Service Contracts are:
   (i) High Risk—Background Investigation (BI).
   (ii) Moderate Risk—Moderate Background Investigation (MBI).
(2) Investigative requirements for IT Service Contracts are:
   (i) High Risk IT—Background Investigation (BI).
   (ii) Moderate Risk IT—Background Investigation (BI).
(b) In addition to the investigations noted above, non-U.S. citizens must have a pre-appointment check that includes an Immigration and Customs Enforcement agency check.
(c) Additional Requirements for Foreign Nationals (Non-U.S. Citizens). To be employed under this contract within the United States, non-U.S. citizens must have:
   (1) Official legal status in the United States;
   (2) Continuously resided in the United States for the last two years; and
   (3) Obtained advance approval from the servicing Security Officer of the contracting operating unit in consultation with the DOC Office of Security (OSY) headquarters. (OSY routinely consults with appropriate agencies regarding the use of non-U.S. citizens on contracts and can provide up-to-date information concerning this matter.)
(d) Security Processing Requirement. Processing requirements for High and Moderate Risk Contracts are as follows:

1. The contractor must complete and submit the following forms to the Contracting Officer's Representative (COR):
   i. Standard Form 85P (SF-85P), Questionnaire for Public Trust Positions;
   ii. FD-258, Fingerprint Chart with OPM's designation in the ORI Block; and
   iii. Credit Release Authorization.

2. The Sponsor will ensure that these forms have been properly completed, initiate the CD-254, Contract Security Classification Specification, and forward the documents to the cognizant Security Officer.

3. Upon completion of security processing, the Office of Security, through the servicing Security Officer and the Sponsor, will notify the contractor in writing of an individual's eligibility to be provided access to a Department of Commerce facility or Department of Commerce IT system.

4. Security processing shall consist of limited personal background inquiries pertaining to verification of name, physical description, marital status, present and former residences, education, employment history, criminal record, personal references, medical fitness, fingerprint classification, and other pertinent information. For non-U.S. citizens, the Sponsor must request an Immigration and Customs Enforcement agency check. It is the option of the Office of Security to repeat the security processing on any contract employee at its discretion.

(e) Notification of Disqualifying Information. If the Office of Security receives disqualifying information on a contract employee, the COR will be notified. The Sponsor, in coordination with the Contracting Officer, will immediately remove the contract employee from duties requiring access to Departmental facilities or IT systems. Contract employees may be barred from working on the premises of a facility for any of the following:
   1. Conviction of a felony crime of violence or of a misdemeanor involving moral turpitude;
   2. Falsification of information entered on security screening forms or on other documents submitted to the Department;
   3. Improper conduct once performing on the contract, including criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct or other conduct prejudicial to the Government, regardless of whether the conduct was directly related to the contract;
   4. Any behavior judged to pose a potential threat to Departmental information systems, personnel, property, or other assets.

(f) Failure to comply with security processing requirements may result in termination of the contract or removal of contract employees from Department of Commerce facilities or denial of access to IT systems.

(g) Access to National Security Information. Compliance with these requirements shall not be construed as providing a contract employee clearance to have access to national security information.

(h) The contractor shall include the substance of this clause, including this paragraph, in all subcontracts.

1.0122 Physical Security: The contractor shall be responsible for safeguarding all government property provided for contractor use. At the close of each work period, government facilities, equipment, and materials shall be secured.

1.0123 Lock Combinations: The contractor shall establish and implement methods of ensuring that all lock combinations are not revealed to unauthorized persons. The contractor shall ensure that lock combinations are changed when personnel having access to the combinations no longer have a need to know such combinations. These procedures shall be included in the contractor’s Quality Control Plan.
1.0124 Key Control: The contractor shall establish and implement methods of making sure all keys/key cards issued to the contractor by the Government are not lost or misplaced and are not used by unauthorized persons. NOTE: All references to keys include key cards. No keys issued to the contractor by the Government shall be duplicated. The contractor shall develop procedures covering key control that shall be included in the Quality Control Plan. Such procedures shall include turn-in of any issued keys by personnel who no longer require access to locked areas. The contractor shall immediately report any occurrences of lost or duplicate keys/key cards to the Task Manager (TM).

1.0124a In the event keys, other than master keys, are lost or duplicated, the contractor shall, upon direction of the TM, re-key or replace the affected lock or locks; however, the Government, at its option, may replace the affected lock or locks or perform re-keying. When the replacement of locks or re-keying is performed by the Government, the total cost of re-keying or the replacement of the lock or locks shall be deducted from the monthly payment due the contractor. In the event a master key is lost or duplicated, all locks and keys for that system shall be replaced by the Government and the total cost deducted from the monthly payment due the contractor.

1.0124b The contractor shall prohibit the use of Government issued keys/key cards by any persons other than the contractor’s employees. The contractor shall prohibit the opening of locked areas by contractor employees to permit entrance of persons other than contractor employees engaged in the performance of assigned work in those areas, or personnel authorized entrance by the TM.

1.013 Task Manager (TM): The TM is:

Task Manager: Jane Doe, NOAA
Email: jane.doe@noaa.gov
Phone: (301) 000-0000

Alternate Task Manager: John Roe, NOAA
Email: john.roe@noaa.gov
Phone: (301) 111-1111

The TM or delegate monitors all technical aspects of the contract and assists in contract administration. The TM is authorized to perform the following functions: assure that the contractor performs the technical requirements of the contract; perform inspections necessary in connection with contract performance; maintain written and oral communications with the contractor concerning technical aspects of the contract; issue written interpretations of technical requirements, including Government drawings, designs, specifications; monitor contractor's performance and notify the Contracting Officer, COR and contractor of any deficiencies; coordinate availability of government furnished property, and provide site entry and badging of contractor personnel. The TM is not authorized to change any of the terms and conditions of the resulting order.

1.1 General PWS Information

1.10 Conservation of Utilities. The contractor shall instruct employees in utilities conservation practices. The contractor shall be responsible for operating under conditions that preclude the waste of utilities, which include turning off the water faucets or valves after using the required amount to accomplish cleaning vehicles and equipment.

1.11 Post Award Conference/Periodic Progress Meetings: The contractor agrees to attend any post award conference convened by the contracting activity or contract administration office in accordance with Federal Acquisition Regulation Subpart 42.5. The Contracting Officer, Contracting Officer’s Representative (COR), Task Manager (TM), and other Government personnel, as appropriate, may meet periodically with the contractor to review the contractor's performance. At these meetings the Contracting Officer will apprise the contractor of how the government views the contractor's performance and the contractor will apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the government.
1.12 Contract Manager: The contractor shall provide a contract manager who shall be responsible for the performance of the work. The name of this person and an alternate who shall act for the contractor when the manager is absent shall be designated in writing to the Contracting Officer. The contract manager or alternate shall have full authority to act for the contractor on all contract matters relating to daily operation of this contract.

1.13 Processing and Identification of Contractor Employees: Prior to commencing work under this contract, the contractor shall submit or have their employee submit the required security forms and number of copies as informed by the Task Manager. The contractor, when notified that the Government rejected the suitability assessment forms shall either have the rejected forms made compliant and resubmitted or withdraw the employee from consideration from working under this contract.

All contract personnel attending meetings, answering Government telephones, and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. They must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed. Contractor personnel will be required to obtain and wear badges in the performance of this task while on-site at a NOAA facility.

1.14 Quality Assurance: The contractor shall ensure quality assurance in accordance with the approved QAP as applicable to the services performed in accordance with this PWS. The contractor shall develop and implement procedures specific to this requirement to identify, prevent, and ensure non-recurrence of defective services. The contractor’s quality assurance program is the means by which he assures himself that his work complies with the requirement of the task order. At a minimum, the contractor shall develop quality assurance procedures that address the areas identified in Technical Exhibit 1, “Performance Requirements Summary.”

Quality Assurance Surveillance: The government shall evaluate the contractor’s performance under this task order in accordance with the Quality Assurance Surveillance Plan. This plan is primarily focused on what the Government must do to ensure that the contractor has performed in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

Government Remedies: The contracting officer shall pursue remedies for the contractor’s failure to perform satisfactory services or failure to correct non-conforming services in accordance with the terms and conditions of the contract.
PART 2
DEFINITIONS & ACRONYMS

- **Service Oriented Architecture** – A set of components which can be invoked, and whose interface descriptions can be published and discovered.

- **FISMA** – Federal Information Security Management Act

- **ITIL** – Information Technology Infrastructure Library

- **PWS** – Performance Work Statement

- **Contracting Officer’s Representative (COR):** A representative from the requiring activity assigned by the Contracting Officer to perform surveillance and to act as liaison to the contractor.

- **Defective Service.** A service output that does not meet the standard of performance associated with it in the Performance Work Statement.

- **Quality Assurance Surveillance Plan (QASP).** An organized written document specifying the surveillance methodology to be used for surveillance of contractor performance to assure services meets the requirements of the Performance Work Statement.

- **Quality Assurance.** Those actions taken by a contractor to control the performance of services so that they meet the requirements of the PWS.

- **Best Effort:** That effort expended by the contractor to perform within the awarded ceiling price all work specified in this task order (TO) and all other obligations under this TO and the basic contract. This effort includes providing required qualified personnel, properly supervised, and following industry accepted methodologies and other practices. The effort is further characterized by operating at all times with the Government’s best interest in mind, using efficient and effective methods, and demonstrating sound cost control. The effort must be identical to the effort that would be expended if this were a firm-fixed price TO and the contractor’s profits were dependent upon reducing costs while meeting the Government’s requirements in terms and quality and schedule. Failure to provide this required effort may result in the withholding of payment for hours expended that do not qualify as best effort or a reduction in the rate per hour to reflect decreased value of services received.
PART 3
GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, AND SERVICES

3.01 General: The government shall provide, the facilities, equipment, materials, and/or services listed below.

3.02 Equipment: The Government will provide: All necessary IT hardware and software to meet the performance requirements

3.03 Services:

3.031 Utilities. All utilities in the facility will be available for the contractor’s use in performance of duties outlined in this PWS. The contractor shall instruct employees in utilities conservation practices. The contractor shall be responsible for operating under conditions that preclude the waste of utilities.

3.032 Facilities: The Government will furnish the necessary workspace for the contractor staff to provide the support outlined in this PWS to include desk space, telephones, computers and other items necessary to maintain an office environment.
PART 4
CONTRACTOR FURNISHED ITEMS AND SERVICES

4.01 General: Except for those items specifically stated to be government furnished in Part 3, the contractor shall furnish everything required to perform this PWS.

4.02 Secret Facility Clearance: The contractor shall possess or be eligible to receive and maintain a SECRET facility clearance from the Defense Security Service. The contractor’s employees, performing work in support of this contract shall have been granted a SECRET security clearance from the Defense Industrial Security Clearance Office.
PART 5
APPLICABLE PUBLICATIONS

5.01 Publications applicable to this PWS are listed below.

<table>
<thead>
<tr>
<th>Publication</th>
<th>Date</th>
<th>Page(s)</th>
<th>Internet Address</th>
<th>Mandatory/Advisory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of Management and Budget IT Policies</td>
<td>December 2002</td>
<td>All</td>
<td><a href="http://www.whitehouse.gov/omb/egov">http://www.whitehouse.gov/omb/egov</a></td>
<td>Mandatory</td>
</tr>
<tr>
<td>Department of Commerce IT Policies</td>
<td>January 2004</td>
<td>All</td>
<td><a href="http://ocio.os.doc.gov/ITPolicyandPrograms/Policy___Standards/index.htm">http://ocio.os.doc.gov/ITPolicyandPrograms/Policy___Standards/index.htm</a></td>
<td>Mandatory</td>
</tr>
<tr>
<td>NOAA IT Policies</td>
<td>October 2009</td>
<td>All</td>
<td><a href="http://www.cio.noaa.gov/Policy_Programs/ciopol.html">http://www.cio.noaa.gov/Policy_Programs/ciopol.html</a></td>
<td>Mandatory</td>
</tr>
</tbody>
</table>
## TECHNICAL EXHIBIT 1

**Performance Requirements Summary**

<table>
<thead>
<tr>
<th>Item</th>
<th>Performance Objective</th>
<th>Acceptable Quality Level (AQL)</th>
<th>Method of Surveillance</th>
<th>Incentive/Disincentive</th>
<th>Sample Size (optional)</th>
<th>Frequency (optional)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware installed and running correctly</td>
<td>Within 7 business days of the receipt of the equipment at the primary and backup sites</td>
<td>100% Completed</td>
<td>100% Inspection</td>
<td>Incentive = option period considered if funding available and need exists</td>
<td>100%</td>
<td>At the end of the installation of the hardware</td>
</tr>
<tr>
<td>Software installed and running correctly</td>
<td>Within 7 business days of the receipt of the software at the primary and backup sites</td>
<td>100% Completed</td>
<td>100% Inspection</td>
<td>Incentive = option period considered if funding available and need exists</td>
<td>100%</td>
<td>At the end of the installation of the software</td>
</tr>
<tr>
<td>Initial response to urgent tickets</td>
<td>Within 15 minutes during regular business hours</td>
<td>97%</td>
<td>Inspect ticket documentation</td>
<td>Incentive = option period considered if funding available and need exists</td>
<td>100%</td>
<td>Monthly</td>
</tr>
<tr>
<td>Initial response to regular ticket</td>
<td>Within 4 hours of submission during regular business hours</td>
<td>95%</td>
<td>Inspect ticket documentation</td>
<td>Incentive = option period considered if funding available and need exists</td>
<td>100%</td>
<td>Monthly</td>
</tr>
<tr>
<td>Deliver software as defined by the task/project requirements</td>
<td>Address all requirements and adhere to established software coding standards</td>
<td>99%</td>
<td>Code review and/or walkthrough in staging environment</td>
<td>Incentive = option period considered if funding available and need exists. Disincentive = Corrective action plan submitted to TM and COR for review</td>
<td>100%</td>
<td>Reviewed as delivered</td>
</tr>
</tbody>
</table>

Types of Surveillance to select from:

**Random Sampling**: Appropriate for frequently recurring tasks. Evaluate randomly selected samples of the lot to determine the acceptability of the entire lot.

Random Inspection Guide, Method of surveillance, Lot size, Sample size, Performance requirement, Sampling procedure, Inspection procedure

**100 Percent Inspection**: Appropriate for tasks that occur infrequently. Inspect and evaluate performance each time task is performed

**Periodic Surveillance**: Evaluation of samples selected on other than 100% or statistically random basis. *(i.e. monthly, quarterly, semi-annually, etc.)*

**Validated Customer Complaint**: Complaints must be validated.