

Performance Based Statement of Work
Liferay Repository Plug-in Application
Acquisition Research Program
Graduate School of Business & Public Policy
Naval Postgraduate School

- 1.0 Background/Introduction:** The purpose of Acquisition Research Program (ARP) of the Graduate School of Business & Public Policy (GSBPP) at the Naval Postgraduate School (NPS) is to enhance the quality and quantity of scholarly research in defense acquisition. The ARP contributes to relevant and rigorous acquisition research by linking the research needs of various sponsors (e.g., acquisition practitioners and policy-makers) with qualified student and faculty researchers at NPS and at other institutions by means of grant awards. Under the ARP, these researchers perform research projects and issue their findings in a variety of venues, including technical reports, conference presentations and proceedings, external briefings, and journal publications. Since program inception in 2003, the ARP has produced over 1,700 research products (<http://www.acquisitionresearch.net/publications/>), which are supported by a PHP legacy system. The ARP also sponsors the Acquisition Research Symposium which brings 300+ scholars, acquisition policy-makers, practitioners, and students to Monterey, CA each May to discuss the latest developments in acquisition research.
- 2.0 Scope:** Build a Liferay Repository Plug-in application (LRPA) using the PHP legacy system and the NPS reports repository for the Liferay plug-in as base requirements. The purpose of this LRPA is to 1) migrate current data base and content to the NPS Liferay platform and 2) improve search functionality. The contractor is responsible for the Java application architecture, design, site layout/user interface, database design/programming, application launch, testing, documentation and maintenance in accordance with industry, DOD/DON standards and best practices. Historically, the development effort for this kind of plug-in is roughly six (6) weeks with a full-time effort of a single skilled Liferay developer.

3.0 Tasks:

The contractor shall build the Liferay Repository Plug-in Application (LRPA) by performing the following task (s);

3.1 Architecture: The LRPA shall utilize the following platform and integration:

- 3.1.1 Platform: Liferay Portal 6.2 Enterprise Edition, Tomcat, MySQL, running on RedHat Enterprise Linux
- 3.1.2 Provide integration with Liferay's search index and Application Program Interfaces (API)
- 3.1.3 Section 508 and Accessibility Standards

Section 508 requires Federal departments and agencies that develop, procure, maintain, or use electronic and information technology to ensure that Federal employees and members of the public with disabilities have access to and use of information and data, comparable to that of the employees and members of the public without disabilities--unless it is an undue burden to do so.

3.2 Web Application Security

- 3.2.1 The LRPA and development shall follow DOD/DON standards (STIGS) and best practices (OWASP & SWAT) for web application security and user security.

Reference security guidelines.

<http://iase.disa.mil/stigs/Pages/index.aspx>

<http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf>

<http://software-security.sans.org/resources/swat>

3.3 Functional Requirements

- 3.3.1 User Functionality: the LRPA shall provide users with the following:
 - 3.3.1.1 List view of publications with sortable columns for Title, Authors and Date.
 - 3.3.1.2 Search by publication number, author, series, category and keywords
 - 3.3.1.3 View publication record, print and download full report file
- 3.3.2 Administrator Functionality: the LRPA shall allow administrators to:
 - 3.3.2.1 Add/update/delete publication records, including adding fields to the records.
 - 3.3.2.2 Attach full text PDF file to publication records.
 - 3.3.2.3 Export publication records to Excel
 - 3.3.2.4 Import publication records from Excel.
 - 3.3.2.5 Upload and store publication PDFs to Liferay individually or multiple PDFs at a time. Once uploaded, the individual PDFs shall be linked to the publication record and the link shall be maintained.
 - 3.3.2.6 Specify the Liferay site specific to each Publication

3.4 Documentation

- 3.4.1 Prepare a detailed and precise technical specification (application blueprint) document
- 3.4.2 Technical documentation shall include:
 - 3.4.2.1 List of areas where passwords are used.
 - 3.4.2.2 List of each source code file, functionality and how it relates to other files
 - 3.4.2.3 List of libraries used and where and their source site url's
 - 3.4.2.4 Build files (How to build and compile the project)
- 3.4.3 Database documentation: List of Data structures and tables. Minimum meta and configuration data required for the site to run.
- 3.4.4 Inline code documentation: Each class, function should have documentation of what the function is used for and some basic pseudo code steps describing what the function does
- 3.4.5 User Documentation
- 3.4.6 Provide status updates to and align goals with the COR and TPOC weekly.

3.5 Acceptance Testing: The Liferay Repository Plug-in Application should be fit for purpose and mistakes shall be eliminated. LRPA must be populated with the existing report and repository data, users and other data during and all areas should be validated and tested, without bugs. See the Quality Assurance Plan below for testing details.

3.6 Troubleshoot and resolve system bugs as reported in the NPS JIRA issue tracking system

3.7 Transition the Liferay plug-in application to the Government

3.8 Post-deployment support of the Liferay Repository Plug-in Application

4.0 Deliverables:

The contractor shall be responsible for providing the design, development and deployment of the Liferay Repository Plug-in Application with the following deliverables:

1. Technical Specification Document no later than **September 1, 2016**
2. New Application to Test Site no later than **October 15, 2016**
3. New Application to Live Site no later than **November 15, 2016**
4. Review Final Application and Documentation during the period of **December 1 - 31, 2016**
5. Transition Application to the Government during the period of **December 1 - 31 December 2016**
6. Post-Deployment Support of the LRPA – **January 1, 2016 – June 30, 2017**

5.0 Performance Measurement - Quality Assurance Plan

Task	Deliverable that will be inspected	Acceptable Quality Level (AQL):	Method	Frequency
3.1 – 3.7, 4.0	DOD/DON Standards, Best Practices / Section 508 Compliance	DOD/DON Standards include Security Technical Implementation Guides (STIGS) and The Open Web Application Security Project (OWASP) and Security Web Application Technology (SWAT). 100% Performance Expected.	Review	Continuous
3.4, 4.0	Technical Specification Document	MS Word Document which outlines the technical plan or action and specifications which is in alignment with the Government's requirements. 100% Performance Expected.	Review of Document	Upon Completion
4.0	Commit New Application to Test Site with existing data incorporated	Commit new application code to a test site. Complete testing, evaluations, trouble shoot and correct errors. 100% Performance Expected.	Test Application on the Test Site	Upon Completion
4.0	Commit New Application to Live Site	Commit tested application to live site. Complete testing, evaluations, trouble shoot and correct errors. 100% Performance Expected.	Test Application on the Live Site	Upon Completion

4.0	Troubleshoot and Resolve system bugs	Troubleshoot and resolve system bugs as reported in the NPS JIRA issue tracking system Errors/bugs resolved within 24 hours.	NPS JIRA	As needed
4.0	Maintain Application	Maintain application, trouble shoot and correct errors / bugs. Errors/bugs resolved within 24 hours 100% Performance Expected – web application online	Error messages, testing functionality	As needed
4.0	Review final Application with the Government	Review Liferay Repository Plug-in Application Code and Documentation with the Government	Review of Documentation, Code	As needed during the period of December 1-31, 2016
4.0	Transition the Application to the Government	Transition the Liferay Repository Plug-in Application to the Government	Review	As needed during the period of December 1 – December 31, 2016
3.8, 4.0	Post Deployment Support, Maintain Application	Maintain application, trouble shoot and correct errors / bugs. Errors/bugs resolved within 24 hours 100% Performance Expected – web application online	Error messages, testing functionality	As needed

If performance falls below the AQL defined above, the Contracting Officer's Representative (COR) shall document the instance(s), coordinate with the Contracting Officer and advise the Contractor. The Contractor will be requested to review the documentation and provide a written response on how performance will be corrected in the future. Re-performance of any work for failure to perform in accordance with the specified AQL or task requirement shall be completed at the Contractor's own expense and at no additional cost to the Government.

6.0 Minimum Technical Requirements: The contractor is responsible for designing, coding and deploying the application, from layout to function and according to the government's specifications. All work is to be performed in accordance with industry, DOD/DON standards and best practices with a responsive design and streamlined navigation.

The contractor shall provide a midlevel architect and developers with Liferay, Java, PHP, JSP using J2EE / Tomcat, MySQL and Apache experience as specified below:

6.1 Requirements for Developers

- 6.1.1 *****MUST BE A U.S. CITIZEN*****
- 6.1.2 At least 5 years working experience with Java (JDK 1.6+) in a Linux operating system environment
- 6.1.3 At least 3 years working experience in Liferay portal development and implementation.
- 6.1.4 At least 3 years working experience with Liferay Plugin Development and Customization using Liferay Plugins SDK, Liferay APIs, XML, and Java-specific web services including, but not limited to, JSR 168 and JSR 286
- 6.1.5 At least 3 years working developer experience with Java Enterprise technologies (Spring, Hibernate, and Tomcat).
- 6.1.6 At least 2 years of experience with coding HTML, CSS, and JavaScript for multiple browser platforms and operating systems.
- 6.1.7 At least 1 year of working experience with Git
- 6.1.8 At least 1 year of working experience with issue tracking systems, such as JIRA

6.2 Evaluation

- 6.2.1 A one (1) page resume for each team member.
- 6.2.2 A link to a sample of an application built which utilized Java, JSP using J2EE / Tomcat, MySQL and Apache and Liferay. Proposing contracting team must have been the prime and the size of the development team no more than three.
- 6.2.3 Five (5) snippets of the sample code from the application to demonstrate technical capabilities.

7.0 Period of Performance: 1 September 2016 – 31 December 2016 (Base – Design, Develop and Deploy LRPA)
 1 January 2016 – 30 June 2017 (Option – Post-Deployment Support LRPA)

8.0 Place of Performance: The work will be performed at the contractor’s location.

9.0 Government Furnished Property: The Government shall provide computer resources including access to software, data and communication networks, etc. They shall provide initial guidance, technical information, PHP legacy code and subject matter orientation. The Government will provide the contractor access to systems required to complete the assigned tasks. The contractor shall identify and notify the Government of system documentation necessary for the proper performance of this statement of work.

10.0 Work Week and Hours of Operation:

The Contractor shall provide services during normal working hours excluding federal holidays. Normal working hours are 0730-1630, Monday through Friday, unless requirements dictate otherwise. Exceptions can be permitted by the COR upon request and at the COR’s discretion.

Following is a list of holidays observed by the Government.

<u>Name of Holiday</u>	<u>Time of Observance</u>
New Year’s Day	1 January
Martin Luther King Jr. Day	Third Monday in January
President's Day	Third Monday in February
Memorial Day	Last Monday in May
Independence Day	4 July
Labor Day	First Monday in September
Columbus Day	Second Monday in October

Veteran's Day	11 November
Thanksgiving Day	Fourth Thursday in November
Christmas Day	25 December

If any of the above holidays occur on a Saturday or a Sunday, then such holiday shall be observed by the Contractor in accordance with the practice as observed by the assigned Government employees at the using activity

11.0 Travel: Not applicable

12.0 Transition Activities: It is essential to the Government that services required under this PWS are performed without interruption. At the conclusion of any performance period, including option periods or extensions, the services provided under this PWS may be awarded to another contractor. The contractor in place shall be required to assist in the transition activities.

13.0 Security Requirements: Sensitive Unclassified. Security clearance is not required. U.S. citizenship is required.

14.0 Human Subject Research: Contractor personnel performing work under this contract may not support, advise, or conduct research involving human subjects. If at any time during the period of performance of this contract the tasks involve human subject research, the Contractor shall immediately notify the Contracting Officer. The contract must be amended in accordance with DoDD 3216.02 and DFAR 252.235-7004 in the event human subject research is proposed.

15.0 Privacy Act Statement:

“Pursuant to Title 5 United States Code 552a(m)(1), the contractor and all employees of the contractor working under this contract are required to comply with the requirements of 5 U.S.C. 552a (“The Privacy Act of 1974”).”

16.0 Identification of Contractor Employees:

In accordance with DFAR 211.106, there shall be a clear distinction between Government employees and service contractor employees. Service contractor employees shall identify themselves as contractor personnel by introducing themselves or being introduced as contractor personnel. Contractor personnel will be required to obtain and wear badges or other visible identification for meetings with Government personnel to provide a clear distinction between service contractor employees and Government personnel. In addition, contractor personnel shall appropriately identify themselves as contractor employees in telephone conversations and in formal and informal written correspondence. 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.

17.0 Non-Personal Services Statement:

Contractor employees performing services under this order will be controlled, directed, and supervised at all times by management personnel of the contractor. Contractor management will insure that employees properly comply with the performance work standards outlined in the SOW. Contractor employees will perform their duties independent of, and without the supervision of, any Government official or other Defense Contractor. The tasks, duties, and responsibilities set forth in the task order may not be interpreted or implemented in any manner that results in any contractor employee creating or modifying Federal policy, obligating the appropriated funds of the United States Government, overseeing the work of Federal employees, or otherwise violating the prohibitions set forth in Parts 7.5 and 37.1 of the Federal Acquisition Regulation (FAR). The Government will control access to the facility and will perform the inspection and acceptance of the completed work.

18.0 NAVSUP 5252.204-9400 Contractor Unclassified Access to Federally Controlled Facilities, Sensitive Information, Information Technology (IT) Systems or Protected Health Information (July 2013)

Homeland Security Presidential Directive (HSPD)-12, requires government agencies to develop and implement Federal security standards for Federal employees and contractors. The Deputy Secretary of Defense Directive-Type Memorandum (DTM) 08-006 – “DoD Implementation of Homeland Security Presidential Directive – 12 (HSPD-12)” dated November 26, 2008 (or its subsequent DoD instruction) directs implementation of HSPD-12. This clause is in accordance with HSPD-12 and its implementing directives.

APPLICABILITY

This clause applies to contractor employees requiring physical access to any area of a federally controlled base, facility or activity and/or requiring access to a DoN or DoD computer/network/system to perform certain unclassified sensitive duties. This clause also applies to contractor employees who access Privacy Act and Protected Health Information, provide support associated with fiduciary duties, or perform duties that have been identified by DON as National Security Position, as advised by the command security manager. It is the responsibility of the responsible security officer of the command/facility where the work is performed to ensure compliance.

Each contractor employee providing services at a Navy Command under this contract is required to obtain a Department of Defense Common Access Card (DoD CAC). Additionally, depending on the level of computer/network access, the contract employee will require a successful investigation as detailed below.

ACCESS TO FEDERAL FACILITIES

Per HSPD-12 and implementing guidance, all contractor employees working at a federally controlled base, facility or activity under this clause will require a DoD CAC. When access to a base, facility or activity is required contractor employees shall in-process with the Navy Command's Security Manager upon arrival to the Navy Command and shall out-process prior to their departure at the completion of the individual's performance under the contract.

ACCESS TO DOD IT SYSTEMS

In accordance with SECNAV M-5510.30, contractor employees who require access to DoN or DoD networks are categorized as IT-I, IT-II, or IT-III. The IT-II level, defined in detail in SECNAV M-5510.30, includes positions which require access to information protected under the Privacy Act, to include Protected Health Information (PHI). All contractor employees under this contract who require access to Privacy Act protected information are therefore categorized no lower than IT-II. IT Levels are determined by the requiring activity's Command Information Assurance Manager. Contractor employees requiring privileged or IT-I level access, (when specified by the terms of the contract) require a Single Scope Background Investigation (SSBI) which is a higher level investigation than the National Agency Check with Law and Credit (NACLC) described below. Due to the privileged system access, a SSBI suitable for High Risk public trusts positions is required. Individuals who have access to system control, monitoring, or administration functions (e.g. system administrator, database administrator) require training and certification to Information Assurance Technical Level 1, and must be trained and certified on the Operating System or Computing Environment they are required to maintain.

Access to sensitive IT systems is contingent upon a favorably adjudicated background investigation. When access to IT systems is required for performance of the contractor employee's duties, such employees shall in-process with the Navy Command's Security Manager and Information Assurance Manager upon arrival to the Navy command and shall out-process prior to their departure at the completion of the individual's performance under the contract. Completion and approval of a System Authorization Access Request Navy (SAAR-N) form is required for all individuals accessing Navy Information Technology resources. The decision to authorize access to a government IT system/network is inherently governmental. The contractor supervisor is not authorized to sign the SAAR-N; therefore, the government employee with knowledge of the system/network access required or the COR shall sign the SAAR-N as the "supervisor".

The SAAR-N shall be forwarded to the Navy Command's Security Manager at least 30 days prior to the individual's start date. Failure to provide the required documentation at least 30 days prior to the individual's start date may result in delaying the individual's start date.

When required to maintain access to required IT systems or networks, the contractor shall ensure that all employees requiring access complete annual Information Assurance (IA) training, and maintain a current requisite background investigation. The Contractor's Security Representative shall contact the Command Security Manager for guidance when reinvestigations are required.

INTERIM ACCESS

The Navy Command's Security Manager may authorize issuance of a DoD CAC and interim access to a DoN or DoD unclassified computer/network upon a favorable review of the investigative questionnaire and advance favorable fingerprint results. When the results of the investigation are received and a favorable determination is not made, the contractor employee working on the contract under interim access will be denied access to the computer network and this denial will not relieve the contractor of his/her responsibility to perform.

DENIAL OR TERMINATION OF ACCESS

The potential consequences of any requirement under this clause including denial or termination of physical or system access in no way relieves the contractor from the requirement to execute performance under the contract within the timeframes specified in the contract. Contractors shall plan ahead in processing their employees and subcontractor employees. The contractor shall insert this clause in all subcontracts when the subcontractor is permitted to have unclassified access to a federally controlled facility, federally-controlled information system/network and/or to government information, meaning information not authorized for public release.

CONTRACTOR'S SECURITY REPRESENTATIVE

The contractor shall designate an employee to serve as the Contractor's Security Representative. Within three work days after contract award, the contractor shall provide to the requiring activity's Security Manager and the Contracting Officer, in writing, the name, title, address and phone number for the Contractor's Security Representative. The Contractor's Security Representative shall be the primary point of contact on any security matter. The Contractor's Security Representative shall not be replaced or removed without prior notice to the Contracting Officer and Command Security Manager.

BACKGROUND INVESTIGATION REQUIREMENTS AND SECURITY APPROVAL PROCESS FOR CONTRACTORS ASSIGNED TO NATIONAL SECURITY POSITIONS OR PERFORMING SENSITIVE DUTIES

Navy security policy requires that all positions be given a sensitivity value based on level of risk factors to ensure appropriate protective measures are applied. Navy recognizes contractor employees under this contract as Non-Critical Sensitive [ADP/IT-II] when the contract scope of work require physical access to a federally controlled base, facility or activity and/or requiring access to a DoD computer/network, to perform unclassified sensitive duties. This designation is also applied to contractor employees who access Privacy Act and Protected Health Information (PHI), provide support associated with fiduciary duties, or perform duties that have been identified by DON as National Security Positions. At a minimum, each contractor employee must be a US citizen and have a favorably completed NACLIC to obtain a favorable determination for assignment to a non-critical sensitive or IT-II position. The NACLIC consists of a standard NAC and a FBI fingerprint check plus law enforcement checks and credit check. Each contractor employee filling a non-critical sensitive or IT-II position is required to complete:

- SF-86 Questionnaire for National Security Positions (or equivalent OPM investigative product)
- Two FD-258 Applicant Fingerprint Cards (or an electronic fingerprint submission)
- Original Signed Release Statements

Failure to provide the required documentation at least 30 days prior to the individual's start date shall result in delaying the individual's start date. Background investigations shall be reinitiated as required to ensure investigations remain current (not older than 10 years) throughout the contract performance period. The Contractor's Security Representative shall contact the Command Security Manager for guidance when reinvestigations are required.

Regardless of their duties or IT access requirements ALL contractor employees shall in-process with the Navy Command's Security Manager upon arrival to the Navy command and shall out-process prior to their departure at the completion of the individual's performance under the contract. Employees requiring IT access shall also check-in and check-out with the Navy Command's Information Assurance Manager. Completion and approval of a System Authorization Access Request Navy (SAAR-N) form is required for all individuals accessing Navy Information Technology resources. The SAAR-N shall be forwarded to the Navy Command's Security Manager at least 30 days prior to the individual's start date. Failure to provide the required documentation at least 30 days prior to the individual's start date shall result in delaying the individual's start date.

The contractor shall ensure that each contract employee requiring access to IT systems or networks complete annual Information Assurance (IA) training, and maintain a current requisite background investigation. Contractor employees shall accurately complete the required investigative forms prior to submission to the Navy Command Security Manager. The Navy Command's Security Manager will review the submitted documentation for completeness prior to submitting it to the Office of Personnel Management (OPM). Suitability/security issues identified by the Navy may render the contractor employee ineligible for the assignment. An unfavorable determination made by the Navy is final (subject to SF-86 appeal procedures) and such a determination does not relieve the contractor from meeting any contractual obligation under the contract. The Navy Command's Security Manager will forward the required forms to OPM for processing. Once the investigation is complete, the results will be forwarded by OPM to the DON Central Adjudication Facility (CAF) for a determination.

If the contractor employee already possesses a current favorably adjudicated investigation, the contractor shall submit a Visit Authorization Request (VAR) via the Joint Personnel Adjudication System (JPAS) or a hard copy VAR directly from the contractor's Security Representative. Although the contractor will take JPAS "Owning" role over the contractor employee, the Navy Command will take JPAS "Servicing" role over the contractor employee during the hiring process and for the duration of

assignment under that contract. The contractor shall include the IT Position Category per SECNAV M-5510.30 for each employee designated on a VAR. The VAR requires annual renewal for the duration of the employee's performance under the contract.

BACKGROUND INVESTIGATION REQUIREMENTS AND SECURITY APPROVAL PROCESS FOR CONTRACTORS ASSIGNED TO OR PERFORMING NONSENSITIVE DUTIES

Contractor employee whose work is unclassified and non-sensitive (e.g., performing certain duties such as lawn maintenance, vendor services, etc.) and who require physical access to publicly accessible areas to perform those duties shall meet the following minimum requirements:

- Must be either a US citizen or a US permanent resident with a minimum of 3 years legal residency in the United States (as required by The Deputy Secretary of Defense DTM 08- 006 or its subsequent DoD instruction) and
- Must have a favorably completed National Agency Check with Written Inquiries (NACI) including a FBI fingerprint check prior to installation access.

To be considered for a favorable trustworthiness determination, the Contractor's Security Representative must submit for all employees each of the following:

- SF-85 Questionnaire for Non-Sensitive Positions
- Two FD-258 Applicant Fingerprint Cards (or an electronic fingerprint submission)
- Original Signed Release Statements

The contractor shall ensure each individual employee has a current favorably completed National Agency Check with Written Inquiries (NACI) or ensure successful FBI fingerprint results have been gained and investigation has been processed with OPM.

Failure to provide the required documentation at least 30 days prior to the individual's start date may result in delaying the individual's start date. In order to maintain access to required systems, the contractor shall ensure completion of annual Information Assurance (IA) training, monitor expiration of requisite background investigations, and initiate reinvestigations as required.

* Consult with your Command Security Manager and Information Assurance Manager for local policy when IT-III (non-sensitive) access is required for non-US citizens outside the United States.