

Performance Based Statement of Work
Liferay Application Developer
Information Technology and Communications Services
Naval Postgraduate School

- 1.0 Background/Introduction:** The Naval Postgraduate School (NPS) located in Monterey, California supports the U.S. Navy, other military branches, and foreign military services with postgraduate education for personnel. Additionally, NPS provides significant research capabilities to the Department of Defense (DoD). The Information Technology and Communication Services (ITACS) Department at NPS provides information technology (IT) support to the entire school.
- 2.0 Scope:** The Liferay Application Developer shall create new and update existing NPS web applications written in the Java programming language. The contractor will be developing and maintaining Liferay portlet applications, working with end users to set migration schedules, identify features, and provide bug fixes for end users. Java developer services are required for the continued development of features and content in the NPS Liferay web portal.
- 3.0 Tasks:** The contractor shall perform the following task(s) as follows:
- 3.1 Develop Liferay Applications
 - 3.1.1 Develop a new Liferay application to manage software downloads. This will allow NPS students, faculty and staff to download licensed software. The application will allow role-based access for certain users to upload and maintain individual software files and titles. An existing ASP application with Microsoft SQL database will be used as the model for functionality.
 - 3.1.2 Complete development of the HR Academic Jobs application, which allows academic positions to be posted and applied for with attachments. A separate hiring committee reviews each position. This is currently 70% developed and requires additional development and testing.
 - 3.1.3 Complete development of the Faculty Activity Integration application, which synchronizes data exchanges with Digital Measures' web services. A publicly searchable faculty profile will be available on the Liferay portal that pulls the education, research, awards and publications from Digital Measures. Jobs will be scheduled within the application to transfer data from NPS systems into Digital Measures and from Digital Measures into the Liferay portal. This is currently 50% developed and requires additional development and testing.
 - 3.1.4 Develop and maintain the Research Topics currently in production use. Research sponsors use this application to submit potential topics for research. A workflow allows NPS and the sponsor to review and approve faculty proposals to the research topics.
 - 3.1.5 Develop and maintain the Research Summaries application currently in production use. This provides abstracts and metadata on research activity at NPS.
 - 3.1.6 Develop and maintain the Link Scanner application currently in production use that checks for broken web and image links within Liferay site content.
 - 3.1.7 Commit new and modified Java code to the NPS Git repository daily.
 - 3.2 Liferay Enhancements
 - 3.2.1 Develop up to two new designs including CSS, JavaScript and Velocity templates in the NPS Liferay theme as determined by the NPS Web Advisory Board.
 - 3.2.2 Develop and maintain up to 10 Liferay hook plugins that customize the functionality of the portal.
 - 3.2.3 Develop and maintain Asset Display Templates using the Freemarker markup language.
 - 3.3 Support Liferay Portal and Applications
 - 3.3.1 Work with Liferay Support to troubleshoot and resolve issues with the Liferay portal.
 - 3.3.2 Install and test patches provided by Liferay Support.
 - 3.3.3 Work with individual site owners to ensure that applications and patches work correctly.
 - 3.3.4 Troubleshoot and resolve Liferay portal programming bugs as reported in the NPS JIRA issue tracking system.
 - 3.3.5 Work with end users to identify and troubleshoot issues associated with the Liferay portal and applications.
 - 3.3.6 Provide documentation and end user training for applications.
 - 3.3.7 Create a monthly report that provides update on status, work completed, work in progress, short-term goals, and other relevant project information.

4.0 Deliverables

The contractor shall be responsible for preparing deliverables in support of the tasks identified in this SOW.

Task	What will be inspected	Acceptable Quality Level (AQL)	Method	Frequency / Required By
3.1.1	Software download application	NPS students, faculty and staff can download licensed software. Users with role-based access can upload and maintain individual software files and titles. Bug fixes should be resolved within 10 business days.	Functional testing conducted by the COR and the NPS functional teams, inspecting source code in the Git repositories.	Upon completion Version 1.0 required by end of contract
3.1.2	HR Academic Jobs Application	Academic positions are posted and applied for within the application. A list of users can be maintained for the hiring committee of each position. Bug fixes should be resolved within 10 business days.	Functional testing conducted by the COR and the NPS functional teams, inspecting source code in the Git repositories.	Upon completion Version 1.0 required by 31-Dec-2016
3.1.3	Faculty Activity Integration	Faculty Activity data is synchronized with Digital Measures using web services. A publicly searchable faculty profile is available on the Liferay portal that displays the education, research, awards and publications from Digital Measures. Jobs are scheduled to transfer faculty teaching and research data from NPS systems into Digital Measures and from Digital Measures into the Liferay portal. Bug fixes should be resolved within 10 business days.	Functional testing conducted by the COR and the NPS functional teams, inspecting source code in the Git repositories.	Upon completion Version 1.0 required by 31-Jan-2017
3.1.4	Research Topics Application	Research sponsors can submit potential topics for research. A workflow allows NPS and the sponsor to review and approve faculty proposals to the research topics. The forms and configuration are modified to follow the requirements of the research topics workflow. Bug fixes should be resolved within 10 business days.	Functional testing conducted by the COR and the NPS functional teams, inspecting source code in the Git repositories.	As needed
3.1.5	Research Summaries Application	Display searchable abstracts and metadata on research activity at NPS. Bug fixes should be resolved within 10 business days.	Functional testing conducted by the COR and the NPS functional teams, inspecting source code in the Git repositories.	As needed
3.1.6	Link Scanner Application	Liferay site content is scanned for broken web and image links. Bug fixes should be resolved within 10 business days.	Functional testing conducted by the COR and the NPS functional teams, inspecting source code in the Git repositories.	As needed

3.1.7	New and Modified Java Code Git Repository Updates	New and/or modified code has been submitted to the repository.	Inspecting source code in the Git repositories	Weekly
3.2.1	NPS Liferay Theme Design and Design Templates	Liferay Theme maintained and deployed to the production site within 20 business days as determined by NPS web advisory board. Visual design and front-end client capabilities operate without functional or visual defects. Front-end CSS and Javascript must be section 508 compliant.	Functional testing conducted by the COR and the NPS functional teams, inspecting source code in the Git repositories.	2 Designs
3.2.2	Liferay Hook Plugin Customizations	New and updated hook customizations should be resolved within 20 business days of assignment. Bug fixes should be resolved within 10 business days.	Functional testing conducted by the COR and the NPS functional teams, inspecting source code in the Git repositories.	Up to 10
3.2.3	Asset Display Templates	Working Asset Display Templates written in Freemarker markup language that display content according to functional requirements. Bug fixes should be resolved within 10 business days.	Functional testing conducted by the COR and the NPS functional teams.	As needed
3.3	Monthly Reports for Liferay Portal Support and Applications	Details all patches installed and tested, troubleshooting and bug updates, documentation completed, JIRA updates	ITACS JIRA tracking system with COR oversight and functional testing by the NPS functional team	Monthly

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.

5.0 Minimum Technical Requirements:

- Liferay Application Developer (U.S. Citizen)
 - At least 4 years Java Programming Language experience
 - At least 2 years of experience in developing Java web applications for Liferay Portal version 6.2 or Java web applications that adhere to the Java Portlet Specification v1.0 or v2.0 (JSR 168, JSR 268).
 - At least 2 years of experience with enterprise-scale web application development, Struts, OJB, Eclipse or IntelliJ (either is satisfactory), Apache Tomcat, JUnit, log4j, Linux, and MySQL.

- At least 2 years of experience working with XML, WSDL, SOAP, and RESTful web services.
- At least 2 years of experience with coding HTML, CSS, JSP, JSTL, and JavaScript for multiple browser platforms and operating systems.
- At least 2 years of experience with Spring
- At least 2 years of experience with Hibernate
- At least 1 year of experience with Git
- Experience creating section 508 compliant front-end CSS and javascript themes and templates

6.0 Period of Performance:

The period of performance is for a period of one year commencing from the date of the award.

7.0 Place of Performance:

Work will be performed on site at the Naval Postgraduate School, Monterey, CA 93943.

8.0 Government Furnished Property:

The Government shall provide computer resources including access to workstations, printers, software, data, communication networks, etc. The Government shall provide initial guidance, technical information, subject matter orientation, and documentation such as reference manuals and appropriate publications. The Government will provide the contractor with access to the systems and software required to complete the assigned tasks. The contractor shall identify and notify the Government of any system documentation necessary for the proper performance of the aforementioned tasks.

The government shall provide one workstation, and sufficient supplies and equipment to perform all of the required tasks at NPS. Any Government-provided property and information shall be used for official Government business only. Any applicable documents that are authorized for use in the performance of these services shall be provided, in accordance with security and contract terms and conditions.

9.0 Work Week and Hours of Operation:

The Contractor shall provide services during normal working hours excluding federal holidays. Normal working hours are 0800-1630, 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

10.0 Travel:

No travel is required in support of this contract.

11.0 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.

12.0 Security Requirements:

Sensitive Unclassified. Security clearance is not required. U.S. citizenship is required.

13.0 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”).”

14.0 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.

15.0 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.

16.0 Invoice Schedule

Contractor may invoice monthly in arrears.

Invoices shall be submitted once a month for services rendered and travel performed during the previous month. All invoices need to be submitted electronically via WAWF. Hard copy invoices cannot be accepted. Only one invoice may be submitted per month. Invoices must identify the invoicing period. If charges against more than one line item have occurred during the invoicing period, all charges must be combined into one invoice. If invoicing against travel, the invoice must contain a summary detailing the charges as well as an attachment of supporting documentation. The contractor’s failure to include the necessary information or a more frequent invoice submission than authorized will result in invoices being rejected.

17.0 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 a US citizen
- 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.