Source Code Guidelines Acquisition Language - Contracts

Use case 2: Contracts with a need for source code

Updated as of: 6/9/20

DISCLAIMER: This document reflects the policy objectives of the ITS JPO, specifically the ITS JPO Source Code Guidelines, and applies ONLY to research projects funded, either fully or partially, by the ITS JPO. This document may not be suitable for other U.S. DOT or non-U.S. DOT missions. For any questions or concerns regarding the applicability of this document or the ITS JPO Source Code Guidelines, please contact the ITS JPO at data.itsjpo@dot.gov.

I. Introduction:

The ITS JPO Source Code Guidelines outline key requirements to maximize the ITS JPO's return on investment for projects producing source code, including making this source code publicly accessible and open source. To operationalize these requirements, federal projects and solicitations must have procurement language requiring adherence to the relevant portions of the ITS JPO Code Guidelines. The below language lays out requirements for Program Managers and acquisition personnel to input into ITS JPO-funded contracts that will produce source code. This language is meant to be tailored as appropriate for specific procurements and requirements. Projects doing major software development can also contact ITS JPO (data.itsjpo@dot.gov) and the IT Acquisition Center of Excellence for more information on best practices for agile software development contract language to augment this baseline language for all projects producing source code.

ITS JPO Program Managers and acquisition personnel must consider including elements of this language in a procurement if a contract might produce source code, even if it is not an explicit deliverable or deemed necessary at the solicitation stage. In particular, not including the Data Rights portion of this language opens up the U.S. DOT to risk that it will not receive or have appropriate rights to source code developed over the course of a project. If a project is expected to produce data, ITS JPO Program Managers and acquisition personnel must also consider adding procurement language requiring adherence to the ITS JPO Data Access Guidelines as well. This language may overlap in parts with the below language, so ITS JPO Program Managers and acquisition personnel must review all language (source code and data) to make sure it is clear, concise, not duplicative, and obtains appropriate artifacts and requirements for ITS JPO.

II. How to Use This Language

This language is meant to be inserted into ITS JPO procurements for contracts by ITS JPO Program Managers and/or acquisition personnel. For more information on license requirements stated in this language, see the ITS JPO Open License Guide. For more information on the

README, LICENSE, and CONTRIBUTING deliverables requested as part of this language, see ITS JPO's README template.

RFP Section	Source Code Guideline Mapping	Suggested Source Code Language
C - Statement of Work	Preference for existing solutions over custom-developed code	The U.S. DOT encourages contributions to existing, non-proprietary code over the development of new, siloed code bases. The U.S. DOT also prefers hybrid solutions - or those containing a mixture of existing federal, commercial, or open source code and custom-developed code. Projects shall make every attempt to use publicly available data and source code, or data and source code that can be made public, before using proprietary data and source code. Additionally, the U.S. DOT is looking for a Recipient that will use the latest data and source code methodologies and standards accepted by industry and is able to evolve with the latest industry-accepted methodologies and standards throughout the course of the project.
C - Statement of Work	Open Source	The U.S. DOT strongly prefers that the Contractor use, acquire and develop open source technologies throughout the course of the project and that any code developed for the project is open source. Open source is defined as publicly accessible works that can be used, modified, and shared by anyone, and distributed under licenses that comply with the definition of "Open Source" provided by the Open Source Initiative and/or meet the definition of "Free Software" provided by the Free Software Foundation. The priority of open source should be reflected in the Contractor's response.
C - Statement of Work	General Compliance	All work conducted under this contract must comply with all federal, U.S. DOT, ITS JPO, and other applicable policies and guidelines (e.g. the Federal Source Code Policy, U.S. DOT Departmental Source Code Management Memo, and Code.gov guidance) throughout the period of performance of this work, including those at https://its.dot.gov/code/#/source-code-guidelines. The Contractor must also comply with new and updated policies throughout the period of performance, including updates to federal, U.S. DOT and ITS JPO policies and guidelines.

C - Statement of Work	Accessibility, Security and Licensing	The Contractor must make available to the U.S. DOT copies of all work developed in performance with this contract, including but not limited to software and data. Consistent with federal and U.S. DOT policy, all source code developed through this project must be made publicly accessible and developed in the open unless a specific intellectual property, privacy, security or other valid restriction on public access is identified and approved by the U.S. DOT. Where valid restrictions exist, the Contractor must make source code and associated documentation adhere to as many open source and open development principles as possible. This may include making a redacted version of the source code publicly accessible, using an incremental release schedule, or restricting access only to sensitive portions of the code. When made accessible, source code must be available in an open format and use open standards that are platform independent, machine readable, and available to the public for free and without restrictions that would impede the reuse of the source code. The Contractor must assign the Creative Commons Zero (CC0 1.0 Universal) license to all new source code and associated documentation developed in performance of this contract. The assignment of this license must occur when the source code is made publicly available and made explicit to the public. Project teams may retain existing licenses for any preexisting software integrated into project solutions. In the event preexisting software is used, the U.S. DOT only requires that project teams assign CC0 to new federally-funded, custom-developed source code. The Contractor must make all licensing relationships with preexisting software clear in applications and documentation, including README and LICENSE files for associated source code. The Contractor is required to include these obligations in any sub-awards or other related funding agreements. The U.S. DOT expects Contractors to remove Confidential Business Information (CBI) and Personally Identifiable Information (PII) before providing public access to source code. Source code must adhere to all relevant federal and U.S. DOT security policies, including but not limited to FIPS 199, NIST SP 800-37, the DOT Cybersecurity Policy, the DOT Departmental Cybersecurity Compendium, the DOT Privacy Risk Management Policy, DOT Order 1351.19, and PII Breach Notification Controls. Contractors must use source code

		analysis tools or comparable means to analyze the code and/or compiled versions of code and detect and report weaknesses to U.S. DOT.
C - Statement of Work	Storage	The Contractor shall set up necessary software repositories for source code development. These repositories should be set up in a source code storage system that provides an appropriate level of user access, functionality, and source code management. If the U.S. DOT determines that a proposed source code storage system does not provide an appropriate level of user access, functionality and source code management, the Contractor must propose a new system for approval by the U.S. DOT. Contractors should budget for the costs of source code storage, sharing and management as appropriate.
C - Statement of Work / Section I - Contract Clauses	Data Rights	Data rights under this contract shall be in accordance with FAR 52.227-14, Rights in Data.
C - Statement of Work	Retention	Source code and associated metadata and user documentation developed under this contract must be retained and made accessible to the U.S. DOT for a minimum of five years. This retention period begins when the U.S. DOT first receives access to the source code and associated metadata and user documentation.

Section F – Deliveries or Performance	Standards	The Contractor must make the source code and associated documentation cited herein available on the U.S. DOT's website ITS CodeHub (https://www.its.dot.gov/code/) when source code development begins, and any other appropriate website as requested by the U.S. DOT. Note: All materials posted on a U.S. DOT website must be Section 508 compliant. Deliverables for this award include: • Source code, documentation, and testing scripts that meet acceptance criteria as approved by the Government • As required, a new repository with appropriate permissions, documentation, and security and continuously updating this repository • Repository documentation, to include a README, LICENSE, CONTRIBUTING, and any other files deemed necessary. Templates and examples for these materials can be found on ITS CodeHub. All repository documentation must be stored in the same location as the source code and should describe how the source code will be managed during and after the project. This documentation must contain, at a minimum: o A README file, including at a minimum: ▪ Status of the source code (prototype, alpha, beta, release, etc.) ▪ Intended purpose of the source code and description of what the source code does ▪ Expected engagement level (i.e. how frequently the community can expect activity) ▪ Any other relevant technical details on how to build, make, install, or use the software, including dependencies ▪ A Digital Object Identifier (DOI), and recommendation that users of the source code reference that DOI for attribution in derivative works o A LICENSE file, including at a minimum: ▪ Licensing status of the source code ▪ Full text of the open source license or a link to where the license is officially maintained ▪ Explanation of licensing relationships with any preexisting software used with the source code

		○ A CONTRIBUTING file, including at a minimum: ▪ Description of the licensing status of the source code ▪ How contributions by third parties to the source code will be released (e.g., whether they will be released under the same license and whether those contributors waive their rights accordingly) ▪ Description of coding practices and community norms requested of potential contributors
Section L – Instructions, Conditions, and Notices to Offeror's		Contractors should describe how they will adhere to all requirements listed in Section C of this [RFP/RFQ/etc.]. Proposals should budget for the costs of source code storage, sharing and management as appropriate. Proposals must include a description of a Contractor's plan for the overall structure of their source code and what source code storage system(s) the Contractor intends to use, as well as a preliminary README, LICENSE, and CONTRIBUTING file for all source code that explains how the Contractor intends to manage source code developed as part of this project. Templates and examples for these materials can be found on ITS CodeHub. **[No need to duplicate the following requirement if existing language covers PII and CBI marking]** If the submission includes information the Contractor considers to be trade secret or confidential commercial or financial information, the Contractor should do the following: (1) Note on the front cover that the submission ‘‘Contains Confidential Business Information (CBI)’’, (2) mark each affected page ‘‘CBI’’, and (3) highlight or otherwise denote the CBI portions. [funding agency] protects such information from disclosure to the extent allowed under applicable law. If [funding agency] receives a Freedom of Information Act (FOIA) request for the information, [funding agency] will follow the procedures described in the Department's FOIA regulations at 49 CFR part 7.

Section M – Evaluation Factors for Award		• Responses that demonstrate a strong commitment to open source development, publicly available and publicly accessible code in a way that appropriately addresses CBI or PII concerns will be viewed more positively. • A source code structure and storage plan, as well as preliminary README, LICENSE, and CONTRIBUTING files will be evaluated for alignment to the solicitation's goals and adherence to the solicitation's requirements, as well as confidence that the Contractor has thought through all aspects of source code management with the goal of public accessibility in mind.

Applicable Clauses:

- FAR 52.227-14, Rights in Data
- 17 U.S.C. 105, Subject matter of copyright: United States Government works

Sample Performance Requirements **- Note: these must be tailored to fit the needs of specific projects. The below is an example set of Performance Requirements that may be used in projects producing source code**:

Performance Objective	**Performance Standard**	**Performance Threshold**	**Method of Surveillance**
The Contractor shall have high source code quality and security.	The Contractor ensured high code quality and standards adherence and test quality and test coverage.	100% test coverage, score of A in code quality analysis, 0 infected files in virus scan (From draft Agile PWS): New source code developed by this project must earn the following scores on SonarQube.com (https://sonarqube.com/): 90% or higher unit test coverage; Score of A for Bugs; Score of A for Vulnerabilities; Score of A for Code Smells.	ITS CodeHub metrics, security reviews, TOCOR review

The Contractor’s code’s production performance is high.	The Contractor’s code has high performance in production, including high availability, low response time, high usability, high accuracy and lack of defects.	Each month the team will measure the project using the following criteria to assess the performance maturity of the project. Outstanding Number of Issues: Total number of outstanding issues reported to the project. Response Time: Overall time taken to address an issue. Issue Severity: Complexity of the solution taken to address an issue.	Project status reports, issue and resolution tracking and reports, TOCOR review
The Contractor should contribute to a healthy open source community.	The Contractor contributes to a healthy and thriving open source community, increasing the return on investment for their source code.	The health and activity of the community of practice will be gauged using metrics such as: volume of issues; number, diversity and specialization of users that comprise the software ecosystem; the volume and pattern of contributions, release histories (whether frequent and regular or infrequent and sporadic) that are consistent with the intended use of the software and user ecosystem; search engine results or other tools to gauge how much stakeholders are referencing the software; appropriately detailed and up-to-date documentation; measures of user interest and activity such as (in the case of GitHub) watchers, stars and forks; and evidence of quality code contributions including use of the language's common conventions and design patterns, use of a framework rather than building everything from scratch, and use of a package manager.	Source code storage system metrics, TOCOR review

QASP: