Data Access Guidelines Acquisition Language - Grants

Use case 1: Grants and funding agreements with a need for data

Updated as of: 7/9/20

DISCLAIMER: This document reflects the policy objectives of the ITS JPO, specifically the Data Access 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 Data Access Guidelines, please contact the ITS JPO at data.itsjpo@dot.gov.

I. Introduction:

The ITS JPO Data Access Guidelines outline key requirements that increase the ITS JPO's return on investment for collecting or creating data, including making this data publicly accessible. To operationalize these requirements, solicitations for ITS JPO projects producing data must have procurement language requiring adherence to relevant portions of the ITS JPO Data Access Guidelines.

II. How to Use This Language

The below language is meant to be put into ITS JPO-funded grant and funding agreement solicitations that will collect or create data. This language should be tailored and inserted as appropriate for specific procurements. ITS JPO Program Managers and acquisition personnel are anticipated to make the determination of what language should be incorporated for a specific solicitation. It is recommended that as much of this language as possible is incorporated for projects that will collect or create data. For more information on the Data Management Plan deliverables requested as part of this language, see the ITS JPO's Data Management Resources page, including Templates & Instructions.

ITS JPO Program Managers and acquisition personnel must consider including elements of this language in a procurement if a grant or funding agreement *might* collect or create data, even if it is not an explicit deliverable or deemed necessary at the solicitation stage. In particular, all grants and funding agreements should incorporate the Data Rights portion of this language, as not including this section opens up the U.S. DOT to risk that it will not have appropriate rights to data collected or created over the course of a project. If a project is expected to produce source code, ITS JPO Program Managers and acquisition personnel must also consider adding procurement language requiring adherence to the ITS JPO Source Code Guidelines. 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 the ITS JPO.

Notice Section	Data Access Guidelines Requirement	Suggested Data Access Language
A. Program Description	Preference for Existing Publicly Available Data	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.
A. Program Description	Open Source	The U.S. DOT strongly prefers that the Recipient use, acquire and develop open source technologies throughout the course of the project and that any data collected or created for the project is open source. Open source is defined as publicly accessible works (including data) 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 Recipient's response.
B. Federal Award Information	General Compliance	All work conducted under this [grant/agreement] must comply with all federal, U.S. DOT, ITS JPO, and other applicable policies and guidelines (e.g. the OPEN Government Data Act and the U.S. DOT Public Access Plan including those requirements at https://ntl.bts.gov/public-access/how-comply) throughout the period of performance of this work, including those at https://www.its.dot.gov/data/#/resources/guidelines. The Recipient 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.

B. Federal Award Information	Access, Security and Licensing	The Recipient must make available to the U.S. DOT copies of all work developed in performance of this **[grant/agreement]**, including but not limited to software and data. Consistent with federal policy ([OPEN Government Data Act](#)), awardees must provide public access to data collected or created through the project unless a specific intellectual property, privacy, confidentiality, security, or other valid restriction on public access is identified by the U.S. DOT. Where valid restrictions exist, the Recipient must make data and associated documentation adhere to as many public access principles as possible. This may include making a redacted version of the data publicly accessible, using an incremental release schedule, or restricting access only to sensitive portions of the data. The Recipient must assign the Creative Commons Zero (CC0 1.0 Universal) license to all new data and associated documentation collected or created in performance of this **[grant/agreement]**. The assignment of this license must occur when the data is made publicly available and made explicit to the public. Project teams may retain existing licenses for any preexisting data integrated into project solutions. In the event preexisting data, the U.S. DOT only requires that project teams assign CC0 to new federally-funded data. The Recipient must make all licensing relationships with preexisting data or software clear in applications and documentation, including their Data Management Plan (DMP). The Recipient is required to include these obligations in any sub-awards or other related funding agreements. The U.S. DOT expects Recipients to remove Confidential Business Information (CBI) and Personally Identifiable Information (PII) before providing public access to project data. Data 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. Any privacy concerns should be detailed in the project's DMP. Final research results must satisfy the reporting and compliance requirements as set forth in the [U.S.DOT Public Access Plan](#), including, but not limited to, the use of Open Researcher and Contributor ID (ORCID) numbers, the creation and

		maintenance of a research project record in the Transportation Research Board's (TRB) Research in Progress (RiP) database, and the timely and complete submission of all required publications and associated digital datasets as such terms are defined in the U.S. DOT Public Access Plan. Additional information about how to comply with the requirements can be found at: https://ntl.bts.gov/public-access/how-comply.
B. Federal Award Information	Storage	The Recipient should detail where they plan to store the data and for how long in their preliminary and post-award DMP. Data storage systems used to store project data must provide an appropriate level of user access, functionality and data life cycle management. If the Recipient plans to store their data in a non-U.S. DOT managed system, they must demonstrate in their preliminary DMP how this system adheres to or exceeds these requirements. If a non-U.S. DOT system does not provide user access, functionality and data lifecycle management that meets the U.S. DOT's requirements, the U.S. DOT has the right to require the project to use a different data storage system that does adhere to these requirements. Details on how the U.S. DOT may determine if a data storage system is appropriate can be found at https://ntl.bts.gov/public-access/guidelines-evaluating-repositories. Recipients should budget for the costs of data storage, sharing, and management as appropriate.
B. Federal Award Information	Data Rights	Data rights under this [grant/agreement] shall be in accordance with 2 CFR 200.315, Intangible property.
B. Federal Award Information	Retention	Data and associated metadata collected or created under this [grant/agreement] 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 data and associated metadata.

		Consistent with federal policy, the Recipient must use standards to promote data interoperability and openness. Where existing standards are insufficient, the Recipient must describe how they will contribute to the development of new standards. The Recipient must make their data, metadata and associated documentation available on the U.S. DOT's website ITS DataHub (https://www.its.dot.gov/data/) when data creation or collection begins, and any other appropriate website as requested by the U.S. DOT. The Recipient must provide metadata on all project data with federal requirements and ITS DataHub requirements. Note: All materials posted on a U.S. DOT website must be Section 508 compliant. Deliverables for this award include: - Data and documentation that meet acceptance criteria as approved by the Government - A Data Management Plan (DMP) that builds off of the Applicant's preliminary DMP. Templates and instructions for DMPs can be found on ITS DataHub. The DMP should be updated regularly throughout the project and whenever a change to the project's data or data management occurs. The DMP must contain, at a minimum: - A Data Management Plan, including at a minimum: - Project Overview (summary information about the research project and its goals, as well as how the project's data helps the U.S. DOT achieve its goals, etc.) - Data Overview (description of the nature, scope, and scale of the data that will be collected and/or created, etc.) - Data Stewardship (details around maintaining data quality, safeguarding the data, access level, when data will be made available and how often it will be updated etc.) - Access Policies (any access restrictions) - Data Storage and Retention (where and how the data will be stored and retained) - Data Rights - Timing (how frequently the data will be shared and updated)
B. Federal Award Information - Deliverables	Data Standards	

D. Application and Submission Information		Applicants should describe how they will adhere to all requirements listed in Section B [or other relevant section] of this [notice/etc.]. Applications should budget for the costs of data storage, sharing, and management as appropriate. The preliminary DMP must be no longer than 10 pages. Any information beyond 10 pages will not be evaluated. Preliminary DMPs will be evaluated for alignment to the solicitation's goals and adherence to the solicitation's requirements, as well as confidence that the Applicant has thought through all aspects of data management and has appropriate plans to ensure data adheres to all relevant requirements and is made accessible while protecting privacy, confidentiality, and security. Applications should indicate how they expect to use the data they collect to evaluate the impact of their project, recognizing that ultimately this will involve collaboration between the applicant and an independent evaluator. Specifically, an essential element of all applications is a set of performance measures that clearly notes how success with the goals of the proposal will be measured and how the data collected will support those goals. A robust evaluation framework should be provided, including details on how relevant demonstration data will both be collected, stored, and shared, with assurances that there are no contractual or other impediments to sharing data with [funding agency] and the independent evaluator. Templates and examples for these materials can be found on ITS DataHub. [No need to duplicate the following requirement if existing language covers PII and CBI marking] If the submission includes information the Applicant considers to be trade secret or confidential commercial or financial information, the Applicant 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.

E. Application Review Information		• Applications that demonstrate strong commitment to publicly accessible data in a way that addresses confidential business information (CBI) or personally identifiable information (PII) concerns will be viewed more positively. • The preliminary DMP will be evaluated for alignment to the solicitation's goals and adherence to the solicitation's requirements, as well as confidence that the Applicant has thought through all aspects of data management with the goal of public accessibility in mind.

Applicable Clauses:

- 2 CFR 200.315, Intangible property
- 17 U.S.C. 105, Subject matter of copyright: United States Government works