Preservation and Maintenance of Published Research Data

NIST O 5702.00
Issue Date: 11/12/2019
Effective Date: 11/13/2017

I. PURPOSE

This order describes requirements and responsibilities for preservation and maintenance of published research data that is relatively static, i.e., not live-streamed or near-real-time. This "relatively static" research data includes data that is updated or corrected after initial publication, but remains unchanged except for these updates.

II. APPLICABILTY

This order applies to[1,2]

1. All National Institute of Standards and Technology (NIST) employees, including full- and part-time employees, temporary government employees, and special government employees, who publish scholarly and technical material, including data, as part of their employment.
2. All NIST associates engaged in research activities at or for NIST who publish scholarly and technical material, including data, to the extent allowed by law and the terms of the associate's agreement,
3. All NIST employees involved in the awarding and/or oversight of NIST contracts, financial assistance awards, or other agreements.

III. REFERENCE

[1] A non-NIST organization that publishes scholarly and technical material, including data, through activities funded wholly or in part by NIST through a grant, cooperative agreement, contract, or other agreement, must manage public access to published scholarly and technical material, including data, as agreed to by NIST and that organization in the terms and conditions of the grant, cooperative agreement, contract, or other agreement between NIST and the non-NIST organization.

[2] In cases where a NIST employee collaborates with an external researcher without an underlying written agreement, expectations for generating a data management plan (DMP) and providing public access to resulting data and/or code should be discussed at the outset of the collaboration. If NIST has the greater role in the project, the DMP should be generated by NIST in accordance with NIST policies. If the external researcher has the greater role and/or has intellectual property rights over the data and/or code, generation of the DMP and provision of public access to the data and/or code should follow their institution's requirements. If the external researcher does not intend to provide public access but is agreeable to NIST providing access, OU management decides whether NIST will do so. This agreement should be obtained in writing. For more information, see NIST G5702.01, Guidance for Making Non-NIST Data Available Through NIST's Data Management Infrastructure.

- Federal Information Security Management Act (FISMA) of 2002
- NIST P 5700.00 Policy on Managing Public Access to Results of Federally Funded Research
- NIST O 5701.00 Managing Public Access to Results of Federally Funded Research
- NIST O 1801.00 Review of Fundamental Research Communications
- NIST S 1801.02 Review of Data Intended for Publication
- NIST Records Retention Schedule, Section 1a

IV. DEFINITIONS[3]

Authoritative Version: A datafile that is deemed reliable by the researcher and his/her supervisor.

Data Steward: The person who is responsible for uploading data to the NIST data repository and for ensuring that information provided in the EDI is current. The steward may or may not be a principal investigator or a person who generated the data, and there may be more than one steward for a dataset.

Digital Object Identifier (DOI): A string of characters used to identify an object such as an electronic document or dataset.

NIST Data Repositories: Data repositories that have been assessed and authorized by NIST to operate, including, for example, those that house Standard Reference Data, the National Vulnerability Database, and disaster data, as well as the repository associated with NIST's Enterprise Data Inventory.

NIST Enterprise Data Inventory (EDI): A searchable system containing a comprehensive listing of NIST datasets with associated metadata, including an indication of whether they may be made publicly available (i.e., release is permitted by law, regulation and policy, subject to all privacy, confidentiality, security, and other valid requirements) and whether they are currently available to the public.

Published Data: Data that is made available to the public, either as part of a scholarly publication or as a stand-alone dataset. In either case, it has been reviewed and approved consistent with NIST O 1801.00 Review of Fundamental Research Communications and S 1801.02 Review of Data Intended for Publication. Published data does not include data made available through limited distribution, e.g., to a group of collaborators.

Research Data: The recorded factual material commonly accepted in the scientific community as necessary to validate research findings, but not any of the following: preliminary analyses, drafts of scientific papers, plans for future research, peer reviews, or

[3] All definitions are in the context of this directive and are listed in alphabetical order. In cases where a definition is adopted from a reference, the reference is cited in a footnote.

communications with colleagues. This "recorded" material excludes physical objects (e.g., laboratory samples). Research data also does not include:

(i) Trade secrets, commercial information, materials necessary to be held confidential by a researcher until they are published, or similar information which is protected under law; and

(ii) Personnel and medical information and similar information the disclosure of which would constitute a clearly unwarranted invasion of personal privacy, such as information that could be used to identify a particular person in a research study.[4]

For purposes of this order, NIST considers the contents of laboratory notebooks to be preliminary analyses.

V. REQUIREMENTS

The authoritative version of data that was (1) produced by NIST and that was (2) funded wholly or in part by NIST must be deposited in a NIST data repository to ensure that confidentiality, integrity, and availability are maintained.

Data may be additionally published in non-NIST repositories that are acceptable to the principal investigator's Organizational Unit (OU); the data steward or principal investigator must update the EDI record to provide the location(s) of non-NIST copies. End users can verify the integrity of those copies by comparing them to the authoritative versions in the NIST repository associated with the EDI.

Published data is assigned a DOI.

For data that was produced by an external recipient of NIST funding through a grant, contract, or other agreement, the NIST Program Officer must create a record in the EDI, consistent with terms and conditions of the funding agreement. Additional guidance is provided in PR 5701.00 Managing Public Access to External Research Funded by NIST.

VI. RESPONSIBILITIES

Chief Information Officer (CIO)

- Provides oversight for maintenance of NIST-level information technology infrastructure to support NIST's provision of public access to data through NIST data repositories.
- Ensures security of NIST's EDI and datasets stored in the associated repository in cooperation with the Director, Office of Data and Informatics.
- Provides oversight for maintenance of a method for users of NIST data to verify the integrity of NIST data they obtain from an external location.

[4] 2 C.F.R. §200.315 (e)(3)

Director, Office of Data and Informatics (ODI)

- Maintains and ensures security and integrity of public data dissemination services for datasets stored in the NIST data repository that is associated with NIST's EDI in cooperation with the CIO.
- Ensures that the NIST data repository that is associated with NIST's EDI adheres to preservation standards and best practices.

Director, Information Services Office

- Provides oversight for creation and maintenance of Digital Object Identifiers (DOIs) for published data.

OU Director or Office Director

- Ensures that employees under his/her supervision publish the authoritative version of his/her research data in a NIST data repository and update EDI records appropriately.

Supervisory Employee within an OU or Office within the ADLP Directorate

- Ensures that EDI records are updated and maintained when employees depart, e.g., by assigning a new data steward if appropriate.

Data Steward

- Follows requirements of NIST O 5701.00 Managing Public Access to Results of Federally Funded Research for providing metadata to the EDI.
- Follows requirements of NIST O 1801.00 Review of Fundamental Research Communications and S 1801.02 Review of Data Intended for Publication for review and approval of fundamental research communications prior to publication.
- Publishes the authoritative version of data in a NIST data repository.
- May publish data in additional repositories.
- Updates EDI record to show location(s) of additional deposits if data has been published in additional repositories.

Federal Program Officer for NIST-Funded External Scientific Research

- Creates a record in the EDI for the data generated through NIST-funded scientific research, consistent with terms and conditions of the funding agreement.

VII. DIRECTIVE OWNER

602 – Special Programs Office

VIII. APPENDICIES

A. Revision History

APPENDIX A

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial	1/4/2016	Katherine Sharpless	Initial draft
Rev. .01	8/7/2017	Dan Cipra	Formatting updates Only
Rev. .02	11/7/2017	Katherine Sharpless	DRB Meeting updates
Rev. .03	11/8/2019	Katherine Sharpless	Clarified responsibilities for providing public access to results from collaborations