Managing Public Access to Results of Federally Funded Research

NIST O 5701.00
Effective Date: 6/26/2015

I. PURPOSE

This order describes requirements and responsibilities for managing public access to results of scientific research funded wholly or in part by NIST.

II. APPLICABILTY

This order applies to:[1]

1. All NIST employees, including full- and part-time employees, temporary government employees, and special government employees, who record factual material commonly accepted in the scientific community as necessary to validate research findings as part of their employment.
2. All 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.
3. All NIST associates engaged in research activities at or for NIST who record factual material commonly accepted in the scientific community as necessary to validate research findings, to the extent allowed by law and the terms of the associate's agreement.
4. All NIST associates engaged in research activities at or for NIST who publish scholarly and technical material, that may include data, to the extent allowed by law and the terms of the associate's agreement,
5. All NIST employees involved in the awarding and/or oversight of NIST contracts, financial assistance awards, or other agreements.
6. All NIST employees involved in the drafting, negotiation, implementation and oversight of agreements under which NIST employees perform research for other parties.

III. REFERENCE

- NIST P 5700.00 NIST Policy on Managing Public Access to Results of Federally Funded Research

[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.

IV. DEFINITIONS[2,]

Accepted Manuscript:[3] The version of a journal article that has been accepted for publication in a journal.

Data: Research data means 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 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.

Data Management Plan (DMP): A defined plan for the management of data that provides, at a minimum, a summary of activities for data generation, a summary of the types of data generated by the relevant activities, the plans for preservation of the generated data, and a description of the appropriate level of access for the generated data.

Digital Object Identifier (DOI): A string of characters used to identify an object such as an electronic document. A group of digital objects may be associated with a Persistent Identifier (*see* Persistent Identifier definition below).

Discoverability: the ability of a piece of content or information to be found.

Federal Digital System (FDSys): A system within the U.S. Government Printing Office (GPO) that will serve as NIST's repository for NIST Technical Series publications as well as other papers that have not been reviewed through an external publisher's peer-review process (e.g., conference proceedings, reports); http://www.gpo.gov/fdsys/.

Final Published Article: The version of record[4]; the publisher's authoritative copy of the final manuscript, including all modifications resulting from the journal's review process, copyediting, stylistic edits, and formatting.

Metadata: Standardized descriptive values that explain, locate, or enable the retrieval of data or publications. (*See*, for example, https://project-open-data.cio.gov/v1.1/schema/.) This does not include 'domain metadata' which provides the user with common understanding of

[2] 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.
[3] National Information Standards Organization, *Journal Article Versions (JAV): Recommendations of the NISO/ALPSP JAV Technical Working Group*, 2008.
[4] 2 C.F.R. §200.315 (e)(3)

the meaning or semantics of the data, to ensure correct and proper use and interpretation of the data by its owners and users.

NIST Editorial Review Board (ERB): The NIST ERB is a Standing Administrative Committee as defined in NIST O 1005.00, NIST Administrative Committees, and currently comprises separate Editorial Review Boards located at Boulder (BERB), JILA (JERB), and Gaithersburg (WERB).

NIST Editorial Review System (ERS): The NIST ERS is the program through which manuscripts are reviewed and approved prior to submission by the author to a publisher.

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.

NIST Public Access Archive System: *See* definitions of PubMed Central and Federal Digital System.

NIST Scholarly and Technical Publications: Publications, including final published articles and the NIST Technical Series publications, which describe the results of NIST technical activities.

NIST Technical Series Publications: NIST scholarly and technical publications published by or for NIST; http://www.nist.gov/nvl/nist_series_publications.cfm.

Open Access: Unrestricted online access to a scholarly or technical publication.

Persistent Identifier: A unique label for a data resource.

PubMed Central (PMC): PubMed Central, maintained by the National Institutes of Health. Beginning October 1, 2015, this platform will serve as NIST's repository for peer-reviewed publications; http://www.ncbi.nlm.nih.gov/pmc/.

V. REQUIREMENTS

1. Data

a. Data Management Plans (DMPs). The requirements stated below are the minimum requirements for DMPs. A NIST Organizational Unit (OU) or Office may expand these requirements to meet the needs of activities within that OU or Office or across OUs or Offices.

NIST OU Directors and Office Directors are responsible for ensuring that DMPs are developed and maintained for all data generated in their respective OU or Office. Responsibility for the development and maintenance of the DMPs may be delegated as determined by the OU Director or Office Director.

In cases where multiple OUs or Offices share a common data-generating activity, the Director of the OU or Office with the greatest role in directing the activity, i.e., the

champion, will determine whether to develop one DMP or multiple DMPs specific to that activity in a manner determined by the champion.

An OU Director or Office Director must ensure that development and maintenance of DMPs is included in performance plans for NIST employees within their OU or Office who have those responsibilities.

All research data generated that results from activities funded wholly or in part by NIST must be covered by a relevant DMP. These plans must contain, at a minimum, the following elements:

(1) Summary of activities: a summary of activities that generate data.

(2) Data types and classification: a summary of the data types generated by the identified activities. *Data should be categorized, at a minimum, according to the data categories presented in the NIST Data Taxonomy and Actions/Consequences for Data Categories, provided in Appendix A of this Order, as applicable*.

(3) Preservation: a plan for storage and maintenance of the data generated by the identified activities, in both the short-term and long-term (if relevant). *Data should be preserved, at a minimum, according to the preservation consequence levels defined in the NIST Data Taxonomy and Actions/Consequences for Data Categories, provided in Appendix A of this Order, as applicable, and in accordance with applicable records retention requirements*.

(4) Review, Discoverability, and Access: a plan describing whether and how the data generated by the identified activities will be reviewed and made available to the public and how the metadata describing it will be entered into the NIST Enterprise Data Inventory (EDI). The plan should describe any known access restrictions for the data and/or metadata, if appropriate. *Data should be made discoverable, at a minimum, according to the discoverability consequence levels defined in the NIST Data Taxonomy and Actions/Consequences for Data Categories, provided in Appendix A, as applicable.*

b. NIST Enterprise Data Inventory (EDI). All metadata for NIST data, as applicable, must be entered into the NIST EDI based on the discovery consequence levels (*see* Appendix A, Section III.3. of this Order) and OU or Office guidance.

2. NIST Scholarly and Technical Publications. All NIST scholarly and technical publications with a publication date of October 1, 2015 or later must be submitted to the NIST public access archive system (*see* Section IV. Definitions) no later than 12 months following publication.

VI. RESPONSIBILITIES

1. NIST Director

(1) Controls and manages NIST's Policy and Order on Managing Public Access to Results of Federally Funded Research.

(2) Ensures coordination of the management of public access to results of federally funded research with non-NIST organizations, as applicable.

2. Associate Director for Laboratory Programs (ADLP)

(1) Implements and provides oversight for maintenance of, and compliance with, NIST's Policy and Order on Managing Public Access to Results of Federally Funded Research.

(2) Ensures the availability of appropriate resources for managing public access to results of federally funded research.

(3) Reviews, approves, and evaluates the effectiveness of NIST OU and Office plans for managing public access to results of federally funded research

(4) Coordinates collaboration and cooperation on implementation of the NIST's Policy and Order on Managing Public Access to Results of Federally Funded Research across NIST and with the Department of Commerce and other federal agencies.

(5) With the Associate Director for Management Resources (ADMR) and the Associate Director for Innovation and Industry Services (ADIIS), coordinates with relevant OUs and Offices in their infrastructure planning and implementation to promote interoperability across NIST.

(6) Oversees the activities of the Directors of the Operating Units within the ADLP Directorate in supporting NIST's Policy and Order on Managing Public Access to Results of Federally Funded Research, as applicable.

3. Associate Director for Management Resources

(1) Facilitates the provision of NIST-level infrastructure to manage public access to results of federally funded research.

(2) Ensures the development and deployment of training, awareness, and outreach activities pertaining to the management of public access to results of federally funded research.

(3) With the ADLP and ADIIS, coordinates with relevant OUs and Offices in their infrastructure planning and implementation to promote interoperability across NIST.

(4) Oversees the activities of the Chief Information Officer and the Directors of the Information Services Office and Office of Acquisition and Agreements Management in supporting NIST's Policy and Order on Managing Public Access to Results of Federally Funded Research, as applicable.

4. Associate Director for Innovation and Industry Services

(1) Oversees the activities of the Directors of the Advanced Manufacturing National Program Office, the Baldrige Performance Excellence Program, the Economic Analysis Office, the Hollings Manufacturing Extension Partnership Program, the Technology Innovation Program, and the Technology Partnerships Office in supporting NIST's Policy and Order on Managing Public Access to Results of Federally Funded Research, as applicable.

5. Chief Information Officer (CIO)

(1) Manages NIST-level information technology infrastructure to support NIST's provision of public access to results of federally funded research.

(2) Ensures that the NIST EDI is available to NIST employees and that NIST inventory records are provided to the Department of Commerce and government-wide inventories in the necessary format, per Office of Management and Budget requirements.

(3) Supports NIST OU Directors' and Office Directors' responsibilities (*see* Section VI.8. of this Order), as applicable.

6. Director, Information Services Office

(1) Works with the Office of Information Systems Management (OISM) to ensure implementation and operation of the NIST EDI.

(2) Manages creation and maintenance of persistent identifiers for NIST Technical Series Publications.

(3) Provides consultation and educational materials for NIST employees on:

a. managing data and providing public access to results of federally-funded research, including use of the NIST EDI, and

b. the NIST review process, as applicable, for results of federally funded research that are intended for dissemination in any media in accordance with Administrative Manual Subchapter 4.09, NIST Technical Communications Program.

(4) Facilitates search and access to metadata for NIST data or final published articles or NIST Technical Series Publications for the public.

(5) Supports NIST OU Directors' and Office Directors' responsibilities (*see* Section VI.8. of this Order), as applicable.

7. Director, Office of Acquisition and Agreements Management (OAAM)

(1) Works with the Directors of NIST OUs and Offices to ensure that, beginning October 1, 2015, grants, cooperative agreements, contracts, and other agreements through which NIST funds activities, wholly or in part, include requirements for managing data and publications, as specified in the terms and conditions of the grant, cooperative agreement, contract, or other agreement with the non-NIST organization,

consistently with the NIST Policy and Order for Managing Public Access to Results of Federally Funded Research.

8. OU Director or Office Director

(1) Implements ADLP-approved plan to manage public access to results of activities funded wholly or in part by NIST within his/her OU or Office.

(2) Works with other offices, e.g., OISM and the Information Services Office, to manage public access to results of activities funded wholly or in part by NIST.

(3) Reviews data to ensure that no personally or business identifiable information is present and that appropriate protective measures are in place prior to making it publicly available; authority to carry out this responsibility may be delegated to the Division Chief or equivalent, per Administrative Manual Subchapter 4.09, NIST Technical Communications Program.

(4) Ensures that his/her OU or Office prioritizes the discoverability (based on the discovery consequence levels in Appendix A, Section III.3. of this Order) and publication of applicable OU or Office datasets based on stakeholder needs and resources required.

9. Supervisory Employee within an OU or Office within the ADLP Directorate

(1) Ensures activities under his/her direction are in compliance with his/her OU or Office plans to manage public access to results of federally funded research.

(2) Ensures employees under his/her supervision meet employee-level requirements of his/her OU or Office plans to manage public access to results of federally funded research.

(3) Works with OAAM to ensure that, beginning October 1, 2015, grants, cooperative agreements, contracts, and other agreements through which NIST funds activities, wholly or in part, include requirements for managing data and publications, as specified in the terms and conditions of the grant, cooperative agreement, contract, or other agreement with the non-NIST organization, consistently with the NIST Policy and Order for Managing Public Access to Results of Federally Funded Research.

10. Non-Supervisory Employee within ADLP Directorate

(1) Complies with the employee-level requirements of his/her OU or Office plans to manage public access to results of federally funded research: prepares and executes DMPs as specified by the OU or Office plans to manage public access to results of federally funded research, and as applicable,

a. provides metadata for NIST data to the NIST EDI or other publicly available repositories, as applicable,
b. if data are tagged as available to the public in the EDI, provides data in open formats via publicly available repositories or upon request and to the extent feasible, directly to the requestor, free of charge unless otherwise excepted, and

c. provides publications dated October 1, 2015 and later to the NIST public access archive system no later than 12 months following publication.

(2) Works with OAAM to ensure that, beginning October 1, 2015, grants, cooperative agreements, contracts, and other agreements through which NIST funds activities, wholly or in part, include requirements for managing data and publications, as specified in the terms and conditions of the grant, cooperative agreement, contract, or other agreement with the non-NIST organization, include requirements for managing data and publications consistently with the NIST Policy and Order for Managing Public Access to Results of Federally Funded Research.

VII. DIRECTIVE OWNER

600 – Associate Director for Laboratory Programs

VIII. APPENDICES

A. NIST Data Taxonomy and Actions/Consequences for Data Categories

B. Revision History

APPENDIX A

NIST DATA TAXONOMY AND ACTIONS/CONSEQUENCES FOR DATA CATEGORIES

I. PURPOSE

The purpose of this taxonomy is to define a collection of terms and concepts that describe classes and categories scientific data arising from unclassified research and programs funded wholly or in part by NIST[5], as well as policy requirements, actions, and consequences that might apply to those categories as a result of requirements expressed in the Office of Science and Technology Policy (OSTP) Open Data Memorandum, OMB Memorandum M-13-13, and Executive Order 13642. (*See* NIST Policy P 105.01.) In the context of these requirements, research data is defined as "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 communications with colleagues."[6]

Although the categories in the NIST data taxonomy are arranged in a pyramid, they are not strictly hierarchical. Categories range from working data to standard reference data (SRD) (*see* Figure 1). The goal of this document is to achieve a shared understanding of the data management space at NIST, not to make policy choices or to define requirements or recommend procedures. This vocabulary is intended to enable discussions among NIST management and technical staff to support NIST's data management Policy and Order.

[5] 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.

[6] For purposes of this policy, NIST is adopting the definition of "research data" provided in 2 C.F.R. §200.315 (e)(3). http://www.gpo.gov/fdsys/pkg/CFR-2014-title2-vol1/pdf/CFR-2014-title2-vol1-sec200-315.pdf

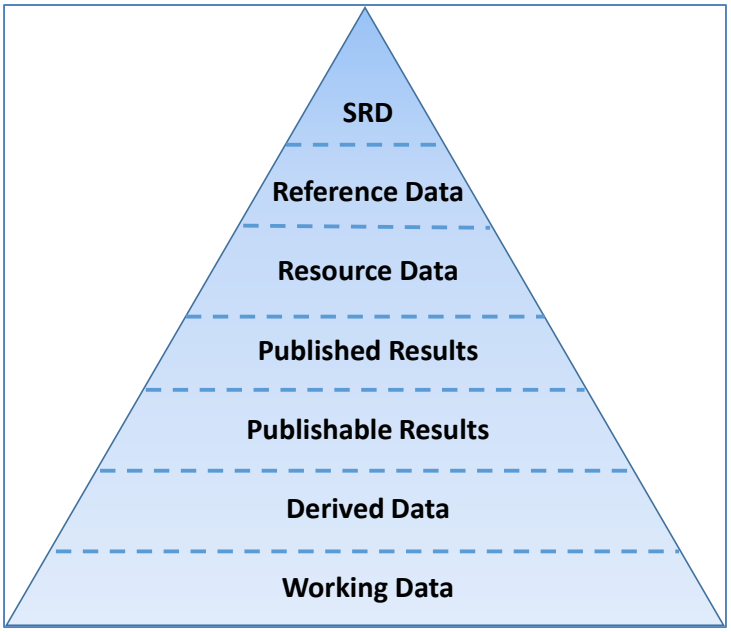


Figure 1. Data pyramid describing the categories of NIST data, ranging from "Working Data" to "Standard Reference Data (SRD)"

II. DATA CATEGORIES

The main categories envisioned for NIST data have been arranged in the form of a "data pyramid," (Figure 1) recognizing that in general the volume of data decreases as you move from the bottom of the pyramid toward the top. This is an oversimplification, and several competing dimensions for characterizing and distinguishing data classes have been combined into this one view for reasons of simplicity and compactness. However, this simplified diagram (Figure 1) provides a useful breakdown of data classes for the narrow context of discussing data management plans and NIST data curation and dissemination policies.

Several classes of data are described in the pyramid, with the following definitions:

1. Working Data

The digital equivalent of entering data in a laboratory notebook. Working data may be raw observational data that is acquired directly from an instrument or a measurement system, or digital values acquired or generated during experiments or simulations. In some cases the researcher responsible for generating the working data may determine that this data has immediate value and is worth preserving, or the researcher may expect that the data will have

value after it has been manipulated or further evaluated, and the data has the potential to develop into a publication or will be used to draw conclusions. In other cases working data may be recognized as not appropriate for broader use in its present form. It may have value to the data producers and their collaborators, but it should be recognized that the data could be easily misinterpreted by people not closely involved in its production because some metadata and important facts about its status or acquisition are not readily available beyond the immediate research team (e.g., adequate metadata for re-purposing is not attached to the data itself, or expending resources to codify needed metadata is not justified, etc.).

2. Derived Data

Underpins the conclusions provided in a publication or report. Derived data comes from working data that has been manipulated, analyzed, processed, or evaluated in some way. The data must have passed some minimal (perhaps *ad hoc*) evaluation and be considered by the responsible researcher (typically the data producer) to be ready for the next steps in the workflow or project/product development effort.

3. Publishable Results

All final or summary results that comply with relevant NIST policies (e.g., SI units, uncertainty statements), that have been reviewed internally and approved by an appropriate NIST authority, and that could be published either in a scientific publication or as a standalone data product.

4. Published Results

Results that are publishable and that are contained in a document that has been reviewed and approved for publication by the necessary NIST organizational authorities, submitted to its intended publisher, and made public.

5. Resource Data

Data used to underpin, support, or defend decisions, actions, or positions of NIST.

6. Reference Data (RD)[7]

Data similar in many characteristics to SRD, sharing features of organization, documentation, and evaluation with SRD. The primary difference between RD and SRD is that reference data is not distributed under the authority of the Standard Reference Data Act

7. Standard Reference Data

Data that has been collected from documented sources, organized, critically evaluated using a procedure that is documented, and distributed, as described in the Standard Reference Data Act. The Standard Reference Data Act defines standard reference data as "quantitative information, related to a measureable physical or chemical property of a substance or system of substances of known composition and structure, which is critically evaluated as to its reliability under [the provisions of the Standard Reference Data Act]."[8] Standard Reference Databases are copyrightable, and NIST may secure copyright in them.

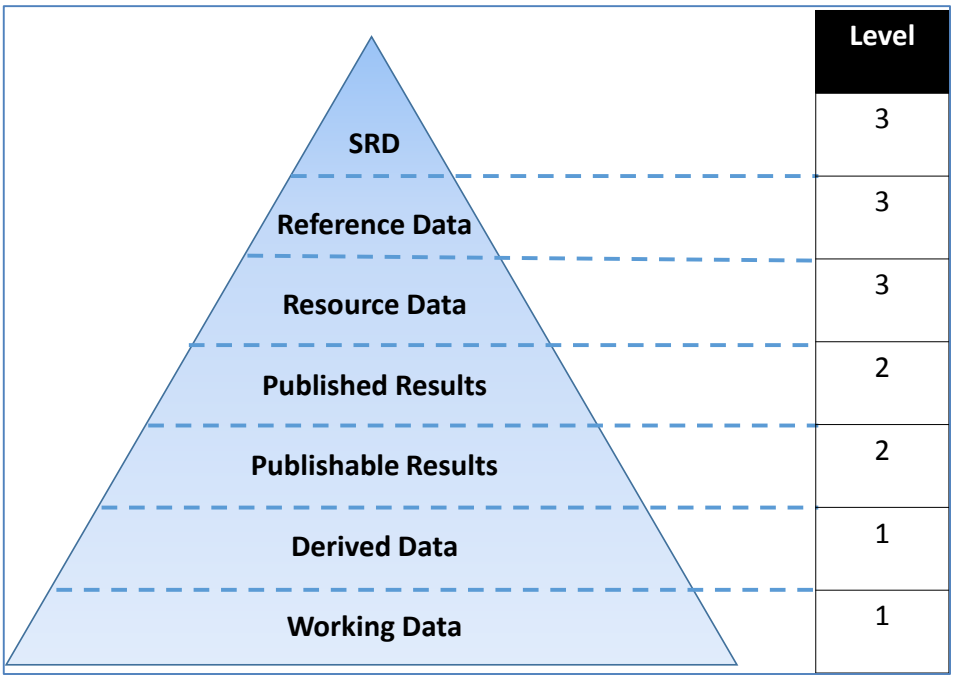
III. ACTION/CONSEQUENCE LEVELS

While the section on Data Categories is intended to define a variety of classes or grades of data that exist at NIST, this section defines corresponding requirements or consequences that should be considered when formulating data policy. As explained earlier, the purpose of this taxonomy document is not to impose these consequences or required actions on the categories, but merely to provide a vocabulary that simplifies discussion of assigning such requirements to various categories. Expressions of NIST data policy (e.g., NIST Directives, Guidance Memoranda, OU policies, etc.) should contain statements that map these consequence levels onto specific categories. Incorporating this taxonomy document as a reference into policy documents that delineate such mappings will simplify those statements of policy and reduce their ambiguity.

[7] It should be noted that the definitions for standard reference data and reference data in this document are similar but not identical to those in the International Vocabulary of Metrology (VIM). There are two key differences: the definition of standard reference data is adopted from the SRD Act, and both definitions are broader than those in the VIM since the VIM only refers to measured data. The VIM defines reference data as being "related to a property of a phenomenon, body, or substance, or to a system of components of known composition or structure, obtained from an identified source, critically evaluated, and verified for accuracy." The scope of reference data as used in this document expands beyond physical and chemical properties.

[8] 15 U.S.C. § 290a, *Standard Reference Data Act*, http://0-www.gpo.gov.librus.hccs.edu/fdsys/pkg/USCODE-1995-title15/pdf/USCODE-1995-title15-chap7A.pdf.

Figure 2. Mapping preservation consequence levels onto the NIST data categories.



1. Preservation Consequence Levels Defined

Consistent with NIST Administrative Manual Subchapter 2.06 Records Management,[9] the NIST Records Retention Schedule[10] for Scientific and Technological Records,[11] and the General Records Schedule[12] for Input Records, Output Records, and Electronic Copies,[13] the following preservation consequence levels correspond to the Data Categories in the data pyramid (*See* Figure 2):

1. No preservation requirements,
2. Individual user responsible for preservation of data,
3. Data must be backed up using a tested/automated process (i.e., proof that restoration is possible).[14]

[9] http://inet.nist.gov/mando/directives/206.cfm
[10] http://inet.nist.gov/mando/nist-records-schedule.cfm
[11] http://inet.nist.gov/mando/services/upload/Items-25-32-Scientific-and-Technological-Records.pdf
[12] http://www.archives.gov/records-mgmt/grs.html
[13] http://www.archives.gov/records-mgmt/grs/grs04-3.pdf
[14] The data are backed up periodically, but the backup frequency is left unspecified and commercial backup technologies such as Tivoli Storage Manager are employed, OR the data are backed up at the level of OISM Central File Services Tier 2, OR the data are backed up at the level of OISM Central File Services Tier 1.

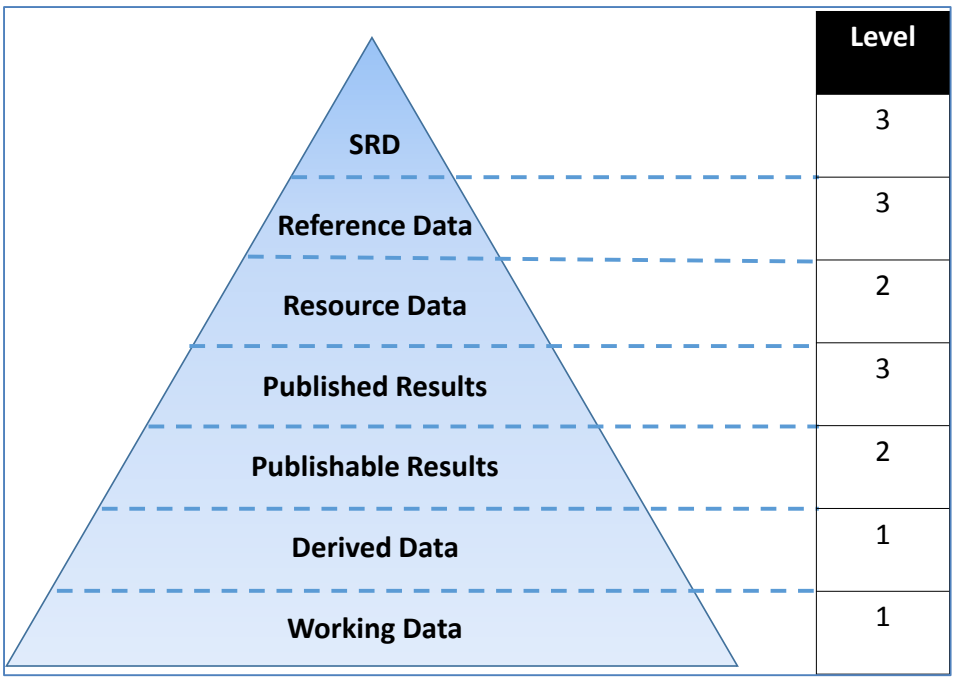


Figure 3. Mapping review consequence levels onto the NIST data categories.

2. Review Consequence Levels Defined

The following review consequence levels correspond to the Data Categories in the data pyramid (*See* Figure 3.):

1. No additional review requirements,
2. Technical aspects of the data must be reviewed and approved within the OU following OU policies.
3. Review by other appropriate NIST authorities (e.g., ERB, ODI) is required.

3. Discoverability Consequence Levels Defined

The following discoverability consequence levels correspond to the Data Categories in the data pyramid (*See* Figure 4.):

1. No discoverability requirements,
2. Metadata values must be entered into the NIST Enterprise Data Inventory (i.e., the NISTXM[15] metadata) and a Persistent Identifier (PID) minted for the dataset,
3. Metadata values in the NIST Enterprise Data Inventory are made publicly accessible.

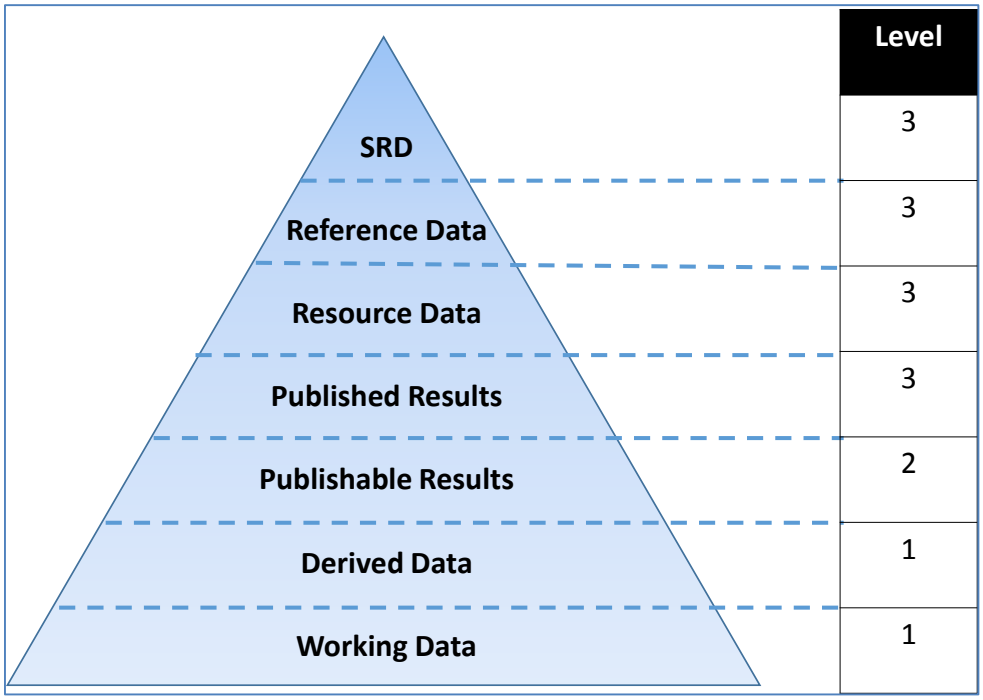


Figure 4. Mapping discoverability consequence levels onto the NIST data categories.

In addition to the guidance above, additional considerations should also be applied by each OU and Office to prioritize the availability of datasets based on factors including stakeholder need, the reasonableness of effort required to make the data available, and other relevant factors.

IV. RELEVANCE OF THE NIST IT SYSTEM SECURITY PLANS

There is a very close relationship between NIST data and the information technology (IT) systems used to store, utilize, and exchange that data. Further, extensive NIST policy governing IT systems has already been defined, and NIST has numerous special publications and Federal Information Processing Standards (FIPS) for the benefit of the nation, pursuant to the Federal

[15] The NIST Extensible Metadata Schema is a definition of the minimum metadata values to be associated with NIST datasets. Formerly known as the "NIST Common Core," the NISTXM is a very minor extension of the OMB-required Common Core metadata fields.

Information Security Management Act (FISMA) of 2002 and other legislation relative to information technology.

Federal law[16] defines the three components of a widely accepted model for discussing information security, including both IT security and information assurance:

a. **Integrity:** guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity;
b. **Confidentiality:** preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
c. **Availability:** ensuring timely and reliable access to and use of information.

This security model applies to information, information *systems*, and related resources (including user information such as research results), and therefore is much broader than just NIST data. However, these concepts are relevant to data generated by federally funded research.

FIPS Publication 199[17] defines three levels of potential impact on organizations and individuals should there be a breach of security (i.e., in this context a loss of confidentiality, integrity, or availability of the data). The potential impact can be LOW, MODERATE, or HIGH if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect, a serious adverse effect, or a severe/catastrophic effect on organizational operations, organizational assets, or individuals. These impact levels are clarified and amplified in FIPS 199. When federally funded research is intended for publication, its INTEGRITY and CONFIDENTIALITY impacts are LOW since the unauthorized modification or disclosure of the data would have a limited adverse effect on NIST operations, assets, and individuals. However, if the federally funded research contains business or personally identifiable information, proprietary information, or other sensitive information prior to publication, CONFIDENTIALITY is deemed MODERATE and therefore requires more stringent security controls. Business or personally identifiable information, proprietary information, or other sensitive information must never be published or otherwise made public. The data categorization and security controls must be documented within the respective NIST OU system security plan**.**

Preservation of records may be accomplished through various means. (NIST staff can see 'How do I backup my data' for more information.)

[16] See 44 U.S.C § 3542 – Definitions.
[17] FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," NIST, February 2004, available at http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

APPENDIX B

REVISION HISTORY

Revision	Date	Responsible Person	Description of Change
Initial	9/18/2014	Katherine Sharpless	Initial release
Rev. .01	4/13/2015	Dan Cipra	Formatting Changes Only
Rec. .02	6/18/2015	Dan Cipra	Incorporated all of the DRB changes