



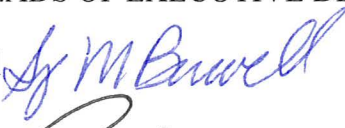
EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D. C. 20503

THE DIRECTOR

May 9, 2013

M-13-13

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Sylvia M. Burwell 
Director

Steven VanRoekel 
Federal Chief Information Officer

Todd Park 
U.S. Chief Technology Officer

Dominic J. Mancini 
Acting Administrator, Office of Information and Regulatory Affairs

SUBJECT: Open Data Policy—Managing Information as an Asset

Information is a valuable national resource and a strategic asset to the Federal Government, its partners, and the public. In order to ensure that the Federal Government is taking full advantage of its information resources, executive departments and agencies (hereafter referred to as “agencies”) must manage information as an asset throughout its life cycle to promote openness and interoperability, and properly safeguard systems and information. Managing government information as an asset will increase operational efficiencies, reduce costs, improve services, support mission needs, safeguard personal information, and increase public access to valuable government information.

Making information resources accessible, discoverable, and usable by the public can help fuel entrepreneurship, innovation, and scientific discovery – all of which improve Americans’ lives and contribute significantly to job creation. For example, decades ago, the Federal Government made both weather data and the Global Positioning System (GPS) freely available to anyone. Since then, American entrepreneurs and innovators have used these resources to create navigation systems, weather newscasts and warning systems, location-based applications, precision farming tools, and much more.

Pursuant to Executive Order of May 9, 2013, *Making Open and Machine Readable the New Default for Government Information*, this Memorandum establishes a framework to help institutionalize the principles of effective information management at each stage of the information’s life cycle to promote interoperability and openness. Whether or not particular information can be made public, agencies can apply this framework to all information resources to promote efficiency and produce value.

Specifically, this Memorandum requires agencies to collect or create information in a way that supports downstream information processing and dissemination activities. This includes using machine-readable and open formats, data standards, and common core and extensible metadata for all new

information creation and collection efforts. It also includes agencies ensuring information stewardship through the use of open licenses and review of information for privacy, confidentiality, security, or other restrictions to release. Additionally, it involves agencies building or modernizing information systems in a way that maximizes interoperability and information accessibility, maintains internal and external data asset inventories, enhances information safeguards, and clarifies information management responsibilities.

The Federal Government has already made significant progress in improving its management of information resources to increase interoperability and openness. The President's Memorandum on *Transparency and Open Government*¹ instructed agencies to take specific actions to implement the principles of transparency, participation, and collaboration, and the Office of Management and Budget's (OMB) *Open Government Directive*² required agencies to expand access to information by making it available online in open formats. OMB has also developed policies to help agencies incorporate sound information practices, including OMB Circular A-130³ and OMB Memorandum M-06-02.⁴ In addition, the Federal Government launched Data.gov, an online platform designed to increase access to Federal datasets. The publication of thousands of data assets through Data.gov has enabled the development of numerous products and services that benefit the public.

To help build on these efforts, the President issued a Memorandum on May 23, 2012 entitled *Building a 21st Century Digital Government*⁵ that charged the Federal Chief Information Officer (CIO) with developing and implementing a comprehensive government-wide strategy to deliver better digital services to the American people. The resulting *Digital Government Strategy*⁶ outlined an information-centric approach to transform how the Federal Government builds and delivers digital services, and required OMB to develop guidance to increase the interoperability and openness of government information.

This Memorandum is designed to be consistent with existing requirements in the Paperwork Reduction Act,⁷ the E-Government Act of 2002,⁸ the Privacy Act of 1974,⁹ the Federal Information Security Management Act of 2002 (FISMA),¹⁰ the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA),¹¹ the Freedom of Information Act,¹² the Information Quality Act,¹³ the

¹ President Barack Obama, Memorandum on Transparency and Open Government (Jan. 21, 2009), available at http://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment.

² OMB Memorandum M-10-06, *Open Government Directive* (Dec. 8, 2009), available at http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf

³ OMB Circular A-130, available at http://www.whitehouse.gov/omb/Circulars_a130_a130trans4/

⁴ OMB Memorandum M-06-02, *Improving Public Access to and Dissemination of Government Information and Using the Federal Enterprise Architecture Data Reference Model* (Dec. 16, 2005), available at <http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-02.pdf>

⁵ President Barack Obama, Memorandum on Building a 21st Century Digital Government (May 23, 2012), available at http://www.whitehouse.gov/sites/default/files/uploads/2012digital_mem_rel.pdf

⁶ Office of Management and Budget, *Digital Government: Building a 21st Century Platform to Better Serve the American People* (May 23, 2012), available at <http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf>

⁷ 44 U.S.C. § 3501 *et seq.*

⁸ Pub. L. No. 107-347, 116 Stat. 2899 (2002) (codified as 44 U.S.C. § 3501 note).

⁹ 5 U.S.C. § 552a.

¹⁰ 44 U.S.C. § 3541, *et seq.*

¹¹ Section 503(a), Pub. L. No. 107-347, 116 Stat. 2899 (2002) (codified as 44 U.S.C. § 3501 note); *see also* Implementation Guidance for Title V of the E-Government Act, Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA), available at http://www.whitehouse.gov/sites/default/files/omb/assets/omb/fedreg/2007/061507_cipsea_guidance.pdf

¹² 5 USC 552(a)(2).

Federal Records Act,¹⁴ and existing OMB and Office of Science and Technology Policy (OSTP) guidance.

If agencies have any questions regarding this Memorandum, please direct them to OMB at datause@omb.eop.gov.

Attachment

¹³ Pub. L. No. 106-554 (2000) (codified at 44 U.S.C. § 3504(d)(1) and 3516). *See also* OMB Memorandum M-12-18, *Managing Government Records Directive* (Aug. 24, 2012), available at <http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-18.pdf>.

¹⁴ 44 U.S.C. Chapters 21, 22, 29, 31, and 33. *See also* 36 CFR Subchapter B - Records Management.

Attachment

This attachment provides definitions and implementation guidance for M-13-13, *Open Data Policy—Managing Information as an Asset*.

I. Definitions:

Data: For the purposes of this Memorandum, the term “data” refers to all structured information, unless otherwise noted.¹⁵

Dataset: For the purposes of this Memorandum, the term “dataset” refers to a collection of data presented in tabular or non-tabular form.

Fair Information Practice Principles: The term “Fair Information Practice Principles” refers to the eight widely accepted principles for identifying and mitigating privacy impacts in information systems, programs and processes, delineated in the National Strategy for Trusted Identities in Cyberspace.¹⁶

Government information: As defined in OMB Circular A-130, “government information” means information created, collected, processed, disseminated, or disposed of, by or for the Federal Government.

Information: As defined in OMB Circular A-130, the term “information” means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

Information life cycle: As defined in OMB Circular A-130, the term “information life cycle” means the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

Personally identifiable information: As defined in OMB Memorandum M-10-23,¹⁷ “personally identifiable information” (PII) refers to information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available (in any medium and from any source) that, when combined with other available information, could be used to identify an individual.

Mosaic effect: The mosaic effect occurs when the information in an individual dataset, in isolation, may not pose a risk of identifying an individual (or threatening some other important interest such as security), but when combined with other available information, could pose such risk. Before disclosing potential PII or other potentially sensitive information, agencies must consider other publicly available data – in

¹⁵ Structured information is to be contrasted with *unstructured* information (commonly referred to as “content”) such as press releases and fact sheets. As described in the *Digital Government Strategy*, content may be converted to a structured format and treated as data. For example, a web-based fact sheet may be broken into the following component data pieces: the title, body text, images, and related links.

¹⁶ The White House, *National Strategy for Trusted Identities in Cyberspace* (April 2011), available at http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

¹⁷ OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications* (June 25, 2010), available at http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf

any medium and from any source – to determine whether some combination of existing data and the data intended to be publicly released could allow for the identification of an individual or pose another security concern.

Open data: For the purposes of this Memorandum, the term “open data” refers to publicly available data structured in a way that enables the data to be fully discoverable and usable by end users. In general, open data will be consistent with the following principles:

- *Public.* Consistent with OMB’s *Open Government Directive*, agencies must adopt a presumption in favor of openness to the extent permitted by law and subject to privacy, confidentiality, security, or other valid restrictions.
- *Accessible.* Open data are made available in convenient, modifiable, and open formats that can be retrieved, downloaded, indexed, and searched. Formats should be machine-readable (i.e., data are reasonably structured to allow automated processing). Open data structures do not discriminate against any person or group of persons and should be made available to the widest range of users for the widest range of purposes, often by providing the data in multiple formats for consumption. To the extent permitted by law, these formats should be non-proprietary, publicly available, and no restrictions should be placed upon their use.
- *Described.* Open data are described fully so that consumers of the data have sufficient information to understand their strengths, weaknesses, analytical limitations, security requirements, as well as how to process them. This involves the use of robust, granular metadata (i.e., fields or elements that describe data), thorough documentation of data elements, data dictionaries, and, if applicable, additional descriptions of the purpose of the collection, the population of interest, the characteristics of the sample, and the method of data collection.
- *Reusable.* Open data are made available under an open license that places no restrictions on their use.
- *Complete.* Open data are published in primary forms (i.e., as collected at the source), with the finest possible level of granularity that is practicable and permitted by law and other requirements. Derived or aggregate open data should also be published but must reference the primary data.
- *Timely.* Open data are made available as quickly as necessary to preserve the value of the data. Frequency of release should account for key audiences and downstream needs.
- *Managed Post-Release.* A point of contact must be designated to assist with data use and to respond to complaints about adherence to these open data requirements.

Project Open Data: “Project Open Data,” a new OMB and OSTP resource, is an online repository of tools, best practices, and schema to help agencies adopt the framework presented in this guidance. Project Open Data can be accessed at <http://project-open-data.github.io>.¹⁸ Project Open Data will evolve over time as a community resource to facilitate adoption of open data practices. The repository includes definitions, code, checklists, case studies, and more, and enables collaboration across the Federal Government, in partnership with public developers, as applicable. Agencies can visit Project Open Data for a more comprehensive glossary of terms related to open data.

¹⁸ Links to the best practices developed in Project Open Data referenced in this memorandum can be found through the directory on this main page.

II. Scope:

The requirements in part III, sections 1 and 2 of this Memorandum apply to all new information collection, creation, and system development efforts as well as major modernization projects that update or re-design existing information systems. National Security Systems, as defined in 40 U.S. C. 11103, are exempt from the requirements of this policy. The requirements in part III, section 3 apply to management of all datasets used in an agency's information systems. Agencies are also encouraged to improve the discoverability and usability of existing datasets by making them "open" using the methods outlined in this Memorandum, prioritizing those that have already been released to the public or otherwise deemed high-value or high-demand through engagement with customers (see part III, section 3.c). Agencies should exercise judgment before publicly distributing data residing in an existing system by weighing the value of openness against the cost of making those data public.

III. Policy Requirements:

Agencies management of information resources must begin at the earliest stages of the planning process, well before information is collected or created. Early strategic planning will allow the Federal Government to design systems and develop processes that unlock the full value of the information, and provide a foundation from which agencies can continue to manage information throughout its life cycle.

Agencies shall take the following actions to improve the management of information resources throughout the information's life cycle and reinforce the government's presumption in favor of openness:

1. **Collect or create information in a way that supports downstream information processing and dissemination activities** – Consistent with OMB Circular A-130, agencies must consider, at each stage of the information life cycle, the effects of decisions and actions on other stages of the life cycle. Accordingly, to the extent permitted by law, agencies must design new information collection and creation efforts so that the information collected or created supports downstream interoperability between information systems and dissemination of information to the public, as appropriate, without the need for costly retrofitting. This includes consideration and consultation of key target audiences for the information when determining format, frequency of update, and other information management decisions. Specifically, agencies must incorporate the following requirements into future information collection and creation efforts:
 - a. **Use machine-readable and open formats**¹⁹ – Agencies must use machine-readable and open formats for information as it is collected or created. While information should be collected electronically by default, machine-readable and open formats must be used in conjunction with both electronic and telephone or paper-based information collection efforts. Additionally, in consultation with the best practices found in Project Open Data and to the extent permitted by law, agencies should prioritize the use of open formats that are non-proprietary, publicly available, and that place no restrictions upon their use.

¹⁹ The requirements of this subsection build upon existing requirements in OMB Statistical Policy Directives No. 1 and No. 2, *available at* <http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/directive1.pdf> and <http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/directive2.pdf>.

- b. **Use data standards** – Consistent with existing policies relating to Federal agencies’ use of standards²⁰ for information as it is collected or created, agencies must use standards in order to promote data interoperability and openness.
 - c. **Ensure information stewardship through the use of open licenses** – Agencies must apply open licenses, in consultation with the best practices found in Project Open Data, to information as it is collected or created so that if data are made public there are no restrictions on copying, publishing, distributing, transmitting, adapting, or otherwise using the information for non-commercial or for commercial purposes.²¹ When information is acquired or accessed by an agency through performance of a contract, appropriate existing clauses²² shall be utilized to meet these objectives while recognizing that contractors may have proprietary interests in such information, and that protection of such information may be necessary to encourage qualified contractors to participate in and apply innovative concepts to government programs.
 - d. **Use common core and extensible metadata** – Agencies must describe information using common core metadata, in consultation with the best practices found in Project Open Data, as it is collected and created. Metadata should also include information about origin, linked data, geographic location, time series continuations, data quality, and other relevant indices that reveal relationships between datasets and allow the public to determine the fitness of the data source. Agencies may expand upon the basic common metadata based on standards, specifications, or formats developed within different communities (e.g., financial, health, geospatial, law enforcement). Groups that develop and promulgate these metadata specifications must review them for compliance with the common core metadata standard, specifications, and formats.
- 2. Build information systems to support interoperability and information accessibility** – Through their acquisition and technology management processes, agencies must build or modernize information systems in a way that maximizes interoperability and information accessibility, to the extent practicable and permitted by law. To this end, agencies should leverage existing Federal IT guidance, such as the *Common Approach to Federal Enterprise Architecture*,²³ when designing information systems. Agencies must exercise forethought when architecting, building, or substantially modifying an information system to facilitate public distribution, where appropriate. In addition, the agency’s CIO must validate that the following minimum requirements have been incorporated into acquisition planning documents and technical design for all new information systems and those preparing for modernization, as appropriate:
- a. The system design must be scalable, flexible, and facilitate extraction of data in multiple formats and for a range of uses as internal and external needs change, including potential uses not accounted for in the original design. In general, this will involve the use of standards and specifications in the system design that promote industry best practices for information

²⁰ See OMB Circular A-119, available at http://www.whitehouse.gov/omb/circulars_a119, and OMB Memorandum M-12-08, *Principles for Federal Engagement in Standards Activities to Address National Priorities* (Jan 27, 2012), available at <http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-08.pdf>

²¹ If a data user augments or alters original information that is attributed to the Federal Government, the user is responsible for making clear the source and nature of that augmentation.

²² See Federal Acquisition Regulation (FAR) Subpart 27.4—Rights in Data and Copyrights, available at https://acquisition.gov/far/current/html/Subpart%2027_4.html

²³ Office of Management and Budget, *Common Approach to Federal Enterprise Architecture*, available at http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/common_approach_to_federal_ea.pdf

sharing, and separation of data from the application layer to maximize data reuse opportunities and incorporation of future application or technology capabilities, in consultation with the best practices found in Project Open Data;

- b. All data outputs associated with the system must meet the requirements described in part III, sections 1.a-e of this Memorandum and be accounted for in the data inventory described in part III section 3.a; and
- c. Data schema and dictionaries have been documented and shared with internal partners and the public, as applicable.

3. Strengthen data management and release practices – To ensure that agency data assets are managed and maintained throughout their life cycle, agencies must adopt effective data asset portfolio management approaches. Within six (6) months of the date of this Memorandum, agencies and interagency groups must review and, where appropriate, revise existing policies and procedures to strengthen their data management and release practices to ensure consistency with the requirements in this Memorandum, and take the following actions:

- a. **Create and maintain an enterprise data inventory** – Agencies must update their inventory of agency information resources (as required by OMB Circular A-130)²⁴ to include an enterprise data inventory, if it does not already exist, that accounts for datasets used in the agency’s information systems. The inventory will be built out over time, with the ultimate goal of including all agency datasets, to the extent practicable. The inventory will indicate, as appropriate, if the agency has determined that the individual datasets may be made publicly available (i.e., release is permitted by law, subject to all privacy, confidentiality, security, and other valid requirements) and whether they are currently available to the public. The Senior Agency Official for Records Management should be consulted on integration with the records management process. Agencies should use the Data Reference Model from the Federal Enterprise Architecture²⁵ to help create and maintain their inventory. Agencies must describe datasets within the inventory using the common core and extensible metadata (see part III, section 1.e).
- b. **Create and maintain a public data listing** – Any datasets in the agency’s enterprise data inventory that can be made publicly available must be listed at [www.\[agency\].gov/data](http://www.[agency].gov/data) in a human- and machine-readable format that enables automatic aggregation by Data.gov and other services (known as “harvestable files”), to the extent practicable. This should include datasets that can be made publicly available but have not yet been released. This public data listing should also include, to the extent permitted by law and existing terms and conditions, datasets that were produced through agency-funded grants, contracts, and cooperative agreements (excluding any data submitted primarily for the purpose of contract monitoring and administration), and, where feasible, be accompanied by standard citation information, preferably in the form of a persistent identifier. The public data listing will be built out over time, with the ultimate goal of including all agency datasets that can be made publicly available. See Project Open Data for best practices, tools, and schema to implement the public data listing and harvestable files.

²⁴ See OMB Circular A-130, section 8(b)(2)(a).

²⁵ Office of Management and Budget, Federal Enterprise Architecture (FEA) Reference Models, available at <http://www.whitehouse.gov/omb/e-gov/fea>

- c. **Create a process to engage with customers to help facilitate and prioritize data release** – Agencies must create a process to engage with customers, through their [www.\[agency\].gov/data](#) pages and other necessary means, to solicit help in prioritizing the release of datasets and determining the most usable and appropriate formats for release.²⁶ Agencies should make data available in multiple formats according to their customer needs. For example, high-volume datasets of interest to developers should be released using bulk downloads as well as Application Programming Interfaces (APIs). In addition, customer engagement efforts should help agencies prioritize efforts to improve the discoverability and usability of datasets that have already been released to the public but are not yet fully “open” (e.g., they are only available in closed, inaccessible formats). See Project Open Data for best practices and tools that can be used to implement customer engagement efforts.
- d. **Clarify roles and responsibilities for promoting efficient and effective data release practices** – Agencies must ensure that roles and responsibilities are clearly designated for the promotion of efficient and effective data release practices across the agency, and that proper authorities have been granted to execute on related responsibilities, including:
 - i. Communicating the strategic value of open data to internal stakeholders and the public;
 - ii. Ensuring that data released to the public are open (as defined in part I), as appropriate, and a point of contact is designated to assist open data use and to respond to complaints about adherence to open data requirements;
 - iii. Engaging entrepreneurs and innovators in the private and nonprofit sectors to encourage and facilitate the use of agency data to build applications and services;
 - iv. Working with agency components to scale best practices from bureaus and offices that excel in open data practices across the enterprise;
 - v. Working with the agency’s Senior Agency Official for Privacy (SAOP) or other relevant officials to ensure that privacy and confidentiality are fully protected; and
 - vi. Working with the Chief Information Security Officer (CISO) and mission owners to assess overall organizational risk, based on the impact of releasing potentially sensitive data, and make a risk-based determination.

- 4. **Strengthen measures to ensure that privacy and confidentiality are fully protected and that data are properly secured** – Agencies must incorporate privacy analyses into each stage of the information’s life cycle. In particular, agencies must review the information collected or created for valid restrictions to release to determine whether it can be made publicly available, consistent with the *Open Government Directive*’s presumption in favor of openness, and to the extent permitted by law and subject to privacy, confidentiality pledge, security, trade secret, contractual, or other valid restrictions to release. If the agency determines that information should not be made publicly available on one of these grounds, the agency must document this determination in consultation with its Office of General Counsel or equivalent.

As agencies consider whether or not information may be disclosed, they must also account for the “mosaic effect” of data aggregation. Agencies should note that the mosaic effect demands a risk-based

²⁶ OMB Statistical Policy Directives 3 and 4 describe the schedule and manner in which data produced by the principal statistical agencies will be released. Statistical Policy Directive No. 4: Release and Dissemination of Statistical Products Produced by Federal Statistical Agencies, *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/omb/fedreg/2008/030708_directive-4.pdf; Statistical Policy Directive 3: Compilation, Release, and Evaluation of Principal Federal Economic Indicators, *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/statpolicy/dir_3_fr_09251985.pdf

analysis, often utilizing statistical methods whose parameters can change over time, depending on the nature of the information, the availability of other information, and the technology in place that could facilitate the process of identification. Because of the complexity of this analysis and the scope of data involved, agencies may choose to take advantage of entities in the Executive Branch that may have relevant expertise, including the staff of Data.gov. Ultimately, it is the responsibility of each agency to perform the necessary analysis and comply with all applicable laws, regulations, and policies. In some cases, this assessment may affect the amount, type, form, and detail of data released by agencies.

As OMB has noted, “The individual’s right to privacy must be protected in Federal Government information activities involving personal information.”²⁷ As agencies consider security-related restrictions to release, they should focus on information confidentiality, integrity, and availability as part of the agency’s overall risk management framework. They are required to incorporate the National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) Publication 199 “Standards for Security Categorization of Federal Information and Information Systems,” which includes guidance and definitions for confidentiality, integrity, and availability.²⁸ Agencies should also consult with the Controlled Unclassified Information (CUI) program to ensure compliance with CUI requirements,²⁹ the National Strategy for Information Sharing and Safeguarding,³⁰ and the best practices found in Project Open Data. In addition to complying with the Privacy Act of 1974, the E-Government Act of 2002, FISMA, and CIPSEA, agencies should implement information policies based upon Fair Information Practice Principles and NIST guidance on Security and Privacy Controls for Federal Information Systems and Organizations.³¹ For example, agencies must:

- a. Collect or create only that information necessary for the proper performance of agency functions and which has practical utility;³²
- b. Limit the collection or creation of information which identifies individuals to that which is legally authorized and necessary for the proper performance of agency functions;³³
- c. Limit the sharing of information that identifies individuals or contains proprietary information to that which is legally authorized, and impose appropriate conditions on use where a continuing obligation to ensure the confidentiality of the information exists;³⁴
- d. Ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information;³⁵ and
- e. Take into account other publicly available information when determining whether particular information should be considered PII (as defined in part I of this Memorandum).

²⁷ See OMB Circular A-130, *available at* http://www.whitehouse.gov/omb/Circulars_a130_a130trans4/

²⁸ NIST FIPS Publication 199 “Standards for Security Categorization of Federal Information and Information Systems”, *available at* <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>

²⁹ Executive Order 13556, Controlled Unclassified Information, *available at* <http://www.whitehouse.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information>.

³⁰ The White House, *National Strategy for Information Sharing and Safeguarding* (December 2011), *available at* <http://www.whitehouse.gov/the-press-office/2012/12/19/national-strategy-information-sharing-and-safeguarding>

³¹ See NIST Special Publication 800-53 “Security and Privacy Controls for Federal Information Systems and Organizations”, *available at* <http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf>

³² See OMB Circular A-130, section 8(a)(2).

³³ See OMB Circular A-130, section 8(a)(9)(b).

³⁴ See OMB Circular A-130, section 8(a)(9)(c).

³⁵ See OMB Circular A-130, section 8(a)(9)(a).

- 5. Incorporate new interoperability and openness requirements into core agency processes –** Consistent with 44 U.S.C. 3506 (b)(2), agencies must develop and maintain an Information Resource Management (IRM) Strategic Plan. IRM Strategic Plans should align with the agency's Strategic Plan (as required by OMB Circular A-11),³⁶ support the attainment of agency priority goals as mandated by the Government Performance and Results Modernization Act of 2010,³⁷ provide a description of how IRM activities help accomplish agency missions, and ensure that IRM decisions are integrated with organizational planning, budget, procurement, financial management, human resources management, and program decisions. As part of the annual PortfolioStat process,³⁸ agencies must update their IRM Strategic Plans to describe how they are meeting new and existing information life cycle management requirements. Specifically, agencies must describe how they have institutionalized and operationalized the interoperability and openness requirements in this Memorandum into their core processes across all applicable agency programs and stakeholders.

IV. Implementation:

As agencies take steps to meet the requirements in this Memorandum, it is important to work strategically and prioritize those elements that can be addressed immediately, support mission-critical objectives, and result in more efficient use of taxpayer dollars.

Agencies should consider the following as they implement the requirements of this Memorandum:

- 1. Roles and Responsibilities –** The Clinger-Cohen Act of 1996 assigns agency CIOs statutory responsibility for promoting the effective and efficient design and operation of all major IRM processes within their agency. Accordingly, agency heads must ensure that CIOs are positioned with the responsibility and authority to implement the requirements of this Memorandum in coordination with the agency's Chief Acquisition Officer, Chief Financial Officer, Chief Technology Officer, Senior Agency Official for Geospatial Information, Senior Agency Official for Privacy (SAOP), Chief Information Security Officer (CISO), Senior Agency Official for Records Management, and Chief Freedom of Information Act (FOIA) Officer. The CIO should also work with the agency's public affairs staff, open government staff, web manager or digital strategist, program owners and other leadership, as applicable.

A key component of agencies' management of information resources involves working closely with the agency's SAOP and other relevant officials to ensure that each stage of the planning process includes a full analysis of privacy, confidentiality, and security issues. Agency heads must also ensure that privacy and security officials are positioned with the authority to identify information that may require additional protection and agency activities that may require additional safeguards. Consistent with OMB Memorandum M-05-08,³⁹ each agency's SAOP must take on a central planning and policy-making role in all agency information management activities, beginning at the earliest stages of planning and continuing throughout the life cycle of the information. In addition, if an agency's SAOP is not positioned within the office of the CIO, the agency should designate an official within the office of the CIO to serve as a liaison to help coordinate with the agency's privacy office.

³⁶ OMB Circular A-11, available at http://www.whitehouse.gov/omb/circulars_all_current_year_all_toc

³⁷ Pub. L. No. 111-352 (2011) (codified as 31 USC § 1120 note).

³⁸ In March 2012 OMB established PortfolioStat accountability sessions, engaging directly with agency leadership to assess the maturity and effectiveness of current IT management practices and address management opportunities and challenges. For FY13 OMB PortfolioStat guidance, see OMB Memorandum M-13-09, *Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management* (Mar. 27, 2013), available at <http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-09.pdf>.

³⁹ OMB Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy* (Feb. 11, 2005), available at <http://m.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-08.pdf>

2. **Government-wide Coordination** – The Federal CIO will work with the United States Chief Technology Officer (CTO) and the Administrator of the OMB Office of Information and Regulatory Affairs (OIRA) to help improve the interoperability and openness of government information. To this end, the Federal CIO will work to establish an interagency working group supported by the Federal CIO Council. The working group should focus on leveraging government-wide communities of practice to help with the development of tools that support information interoperability and openness through repositories such as Project Open Data. Part of this work should be to share best practices related to interoperability and openness within government (e.g., Federal, state, local, and tribal). These collaborations shall be subject to statutory limitations and conducted in a way that fully protects privacy, confidentiality, confidential business information, and intellectual property rights.
3. **Resources** – Policy implementation may require upfront investments depending on the maturity of existing information life cycle management processes at individual agencies. Agencies are encouraged to evaluate current processes and identify implementation opportunities that may result in more efficient use of taxpayer dollars. However, effective implementation should result in downstream cost savings for the enterprise through increased interoperability and accessibility of the agency's information resources. Therefore, these potential upfront investments should be considered in the context of their future benefits and be funded appropriately through the agency's capital planning and budget processes. Some of the requirements in this Memorandum may require additional tools and resources. Agencies should make progress commensurate with available tools and resources.

In addition, tools, best practices, and schema to help agencies implement the requirements of this Memorandum can be found through the Digital Services Innovation Center and in Project Open Data.

4. **Accountability Mechanisms** – Progress on agency implementation of the actions required in this Memorandum will be primarily assessed by OMB and the public through analysis of the agency's updates to IRM plans (part III, section 5), the completeness of the enterprise data inventory (part III, section 3.a), and the data made available in the agency's public data listing (part III, section 3.b).

Nothing in this Memorandum shall be construed to affect existing requirements for review and clearance of pre-decisional information by OMB relating to legislative, budgetary, administrative, and regulatory materials. Moreover, nothing in this Memorandum shall be construed to reduce the protection of information whose release would threaten national security, invade personal privacy, breach confidentiality or contractual terms, violate the Trade Secrets Act,⁴⁰ violate other statutory confidentiality requirements,⁴¹ or damage other compelling interests. This Memorandum is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

⁴⁰ 18 USC § 1905.

⁴¹ See 13 U.S.C. §§ 8, 9 and 301(g) and 22 U.S.C. § 3104.