GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO 2164.2A
10/18/2022

GSA ORDER

SUBJECT: Internal Clearance Process for GSA Data Assets

1. Purpose. This Order provides the internal clearance process that the General Services Administration (GSA) must follow before releasing GSA data assets. GSA IT established this process in collaboration with the Office of the General Counsel (OGC) and the Chief Privacy Officer. The established clearance process ensures timely and improved access to reliable and high-quality data while assuring the privacy, security, and confidentiality of GSA's critical data assets.

The internal clearance process will result in the designation of one of three access levels for each data asset: Public, Restricted Public, or Non-Public.

- **Public (e.g. via data.gov)**: The *data asset is or could be made publicly available to all without restrictions.* The "access level comment" field, a metadata field in GSA's Enterprise Data Inventory (EDI), may be used to provide information on how to remove or reduce technical or resource barriers to public access.

- **Restricted Public (e.g. via D2D)**: The *data asset is available under certain use restrictions.* One example, among many, is a data asset that can only be made available to other Federal agencies, because the data assets contain sufficient detail or linkages that may make it possible to identify individuals, even though the data assets have been stripped of Personally Identifiable Information (PII). This category includes some, but not all, data assets designated by Executive Order 13556 "Controlled Unclassified Information (CUI)" as CUI. The access level comment field must be completed with details on how one can obtain access.

- **Non-Public (e.g. GSA-only)**: The *data asset is not available to members of the public or other Federal agencies*. This category includes data assets that are only available for internal use by GSA, for example confidential budget deliberations. This category might include some, but not all, data assets designated by Executive Order 13556 as CUI. Some non-public data assets may still potentially be available to other intra-agency operating units and/or

other Government agencies, as discussed in OMB Memorandum M-11-02 *Sharing Data While Protecting Privacy* dated November 3, 2010. The access level comment field for non-public data assets must contain an explanation for the reasoning and legal authority behind why these data assets cannot be released.

2. Background. On January 14, 2019, the Open, Public, Electronic and Necessary (OPEN) Government Data Act, as part of the Foundations for Evidence Based Policymaking Act, became law. The OPEN Government Data Act requires federal agencies to publish their information online as open data, using standardized, machine-readable data formats, with their metadata included in the Data.gov catalog.

Under Presidential Executive Order 13642 issued May 9, 2013, *Making Open and Machine Readable the New Default for Government Information*, OMB Memorandum M-19-23 issued July 10, 2019*, Phase 1 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Learning Agendas, Personnel, and Planning Guidance,* and the OPEN Government Data Act, there is an increased demand for data transparency, integration, and sharing across GSA.

GSA's Controlled Unclassified Information policy and this order implement Executive Order 13556, Controlled Unclassified Information (CUI), and the requirements of 32 CFR 2002. CUI is defined as unclassified information that requires safeguarding and dissemination controls pursuant to law, regulation, or Government-wide policy, as listed in the CUI Registry. CUI is authorized for any lawful government purpose, which is any activity, mission, function, or operation that the U.S. Government recognizes as within the scope of its legal authorities.

In addition, OMB Memorandum M-19-18 the *Federal Data Strategy - A Framework for Consistency* issued on June 4, 2019, strives to enable the Federal Government to fully leverage data as a strategic asset. Better access to timely and accurate data within GSA enables better data-driven management and decision-making; increases transparency around business operations; and improves the level of collaboration between GSA, the public and private sectors, and GSA's Federal agency partners. Open access to data also benefits GSA's consolidated investment strategy by allowing more effective decision-making for strategic investments.

3. Cancellation. This Order cancels and supersedes CIO 2164.1 Internal Clearance Process for GSA Data Assets dated September 14, 2015.

4. Revisions. The following updates have been made:

a. Added responsibilities to ensure compliance and protection of sensitive data;

b. Clarified process;

c. Inserted examples of the three access levels; and

d. Updated outdated links and references.

5. Applicability.

a. This Order applies to all GSA employees.

b. This Order applies to the Office of Inspector General (OIG) only to the extent that the OIG determines it is consistent with the OIG's independent authority under the IG Act, and it does not conflict with other OIG policies or the OIG mission.

c. This Order applies to the Civilian Board of Contract Appeals (CBCA) only to the extent that the CBCA determines it is consistent with the CBCA's independent authority under the Contract Disputes Act, and it does not conflict with other CBCA policies or the CBCA mission.

6. Responsibilities.

a. Chief Information Officer (CIO). Is responsible for the overall IT management in GSA.

b. Chief Data Officer (CDO). Has authority and responsibility for, among other things, data governance and lifecycle data management.

c. Chief Privacy Officer (CPO). Oversees GSA's Privacy Program and encourages transparency of GSA operations involving PII.

d. Enterprise Information and Data Management Division (IDEA) Open Data Lead. Manages internal processes to ensure secure clearance processing of GSA data assets prior to release.

(1) Reviews information for valid restrictions prior to release for both internal agency use and external stakeholders in order to ensure proper safeguarding of privacy, security, and confidentiality of controlled unclassified information (CUI);

(2) Documents the law, regulation or government-wide that restricts a data asset or certain components of a data asset from release;

(3) Consults with GSA's Chief Privacy Officer and Technology Law Division (LT) regarding any identified data assets or any portion of data assets that should not be released; and

(4) Encourages dialogue internally to identify more data assets that may be released;

(5) Confirms the data asset does not contain any Controlled Unclassified Information (CUI) data by checking GSA's data catalog systems.

e. Data Stewards. Work with system owners and managers to continually improve agency data. The 'GSA Data Steward' serves as a subject matter expert (SME) and custodian for one or more of their organization's enterprise data assets. A data steward helps other GSA stakeholders better understand and use the data assets to improve their data-driven decision making processes.

f. Domain Stewards. The 'GSA Domain Steward' serves as a subject matter expert (SME) and custodian for one or more of their organization's data domains and the data assets contained within these domains. A domain steward helps other GSA stakeholders better understand and use domain data to improve their data-driven decision making processes. A domain steward oversees all activities falling within their area of expertise. A domain steward has broader knowledge and responsibility than a data steward.

g. System Owners. System owners should work with the data stewards to carry the primary responsibility for defining data requirements. System owners should control access to data as well as oversee changes to data definitions.

7. Process. For secure clearance processing of GSA data assets prior to release, the following sequence of steps must be followed:

a. The System Owner, Data Steward, Domain Steward and/or SSO DEGBs can identify the Services and Staff Office data assets to add to EDI and for possible public release. Refer to CIO 2231.1 GSA Data Release Policy regarding releasing information relating to GSA employees, contractors, and others on whom GSA maintains information.

b. Any data assets that contain information pertaining to OIG must be sent to the Inspector General FOIA Office at OIGFOIA-PrivacyAct@gsaig.gov for a determination to authorize release. The OIG's FOIA process and Public Release process are completely independent of GSA.

c. For data assets not pertaining to OIG, the System Owner or Data Steward requests a spreadsheet template from the IDEA Open Data Lead at opendata@gsa.gov. The requester fills in the metadata and sends it to the Open Data Lead or opendata@gsa.gov. In addition to sending the metadata, the submitter should include the following:

(1) Reasons for possibly restricting release, such as licensing agreements or vendor agreements.

(2) A recommendation regarding the access level -- Public, Restricted Public, or Non-Public (as these terms are defined below).

c. The Data Steward coordinates a review of the information by the relevant Data Evidence Governance Board (DEGB) and program counsel to determine if it can be released to the public in accordance with laws, regulations and government-wide policies.

d. If the data assets are in compliance, the Data Steward will then notify the Open Data Lead who will also conduct a technical review and may coordinate with the Technology Law Division (LT) within OGC and the GSA Privacy Officer, as needed.

e. If the Technology Law Division (LT) or the Privacy Officer does not concur with releasing the data assets, the Data Steward will notify System Owner, Data Steward, Domain Steward and/or SSO DEGBs, and the IDEA Open Data Lead that the data assets package has not cleared review, explain why, and, if possible, suggest necessary revisions.

f. If modifications are needed for release based on findings, the process will start over requiring a new submission of metadata and recommendations as described in 7 a.

g. If there are no suggested modifications from the Technology Law Division (LT) or Privacy Officer, and the data assets are approved only for Restricted Public access (e.g. via D2D) or Non-Public access (e.g. GSA-only), they will be included in the GSA EDI or D2D depending on the level for which they are cleared. If approved for Public access (e.g. via data.gov), the data asset could be made publicly available.

8. References.

a. Project Open Data

b. Data.gov

c. OMB Memorandum M-11-02 - Sharing Data While Protecting Privacy - November 3 2010.

d. Executive Order 13556 - Controlled Unclassified Information - November 4, 2010

e. Building a 21st Century Digital Government - May 23, 2012

f. White House Digital Government Strategy - May 23, 2012

g. Executive Order 13642 - Making Open and Machine Readable the New Default for Government Information - May 9, 2013

h. OMB Memorandum M-13-13 - Open Data Policy - Managing Information as an Asset - May 9, 2013

i. Supplemental Guidance on the Implementation of M-13-13 “Open Data Policy - Managing Information as an Asset”

j. DATA Act (Public Law No. 113-101) - May 9, 2014

k. Appendix A to OMB Circular No. A-123, Management of Reporting and Data Integrity Risk - June 6, 2018

l. Foundations for Evidence-Based Policymaking Act of 2018 (Public Law No: 115-435) - January 14, 2019

m. Federal Data Strategy - A Framework for Consistency - June 4, 2019

n. OMB Memorandum M-19-23 - Phase 1 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Learning Agendas, Personnel, and Planning Guidance - July 10, 2019.

o. CIO 2231.1 GSA Data Release Policy - May 5, 2020

p. CIO 2200.1 GSA Privacy Act Program - May 12, 2020

q. CIO 2103.2 Controlled Unclassified Information (CUI) Policy - April 10, 2021

r. Open Data at GSA

9. Signature.

/S/
DAVID SHIVE
Chief Information Officer
Office of GSA IT