

ENTERPRISE DATA MANAGEMENT POLICY

I. Purpose

This Directive establishes the Department of Homeland Security (DHS) policy on the management of Enterprise Data. Enterprise Data is data created, managed, or maintained within DHS that is common to, or shared among, multiple DHS entities; and data shared outside of DHS in the DHS Information Sharing Environment.

II. Scope

This Directive applies throughout DHS, unless exempted by statutory authority. This Directive applies to all enterprise data regardless of classification unless exempted by statutory authority or regulation.

III. Authorities

- A. Title 5, United States Code (U.S.C.), Section 552a, "Records Maintained On Individuals" (The Privacy Act of 1974)
- B. Title 6, U.S.C., Section 485, "Information Sharing"
- C. Title 44, U.S.C., Chapter 35, "Coordination of Federal Information Policy" (E-Government Act of 2002)
- D. Title 36, Code of Federal Regulations, Part 1236, "Electronic Records Management"
- E. The Office of Management and Budget (OMB), "Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies" (finalized at 67 Federal Regulation 8452, February 22, 2002)
- F. OMB Memorandum M-13-13, "Open Data Policy – Managing Information as an Asset"

- G. Memorandum from the Secretary of DHS to all DHS Components, "DHS Policy for Internal Information Exchange and Sharing," February 1, 2007
- H. DHS Delegation 00002, "Delegation to the Under Secretary for Management"
- I. DHS Delegation 04000, "Delegation for Information Technology"
- J. DHS Directive 142-02, "Information Technology Integration and Management"
- K. DHS Directive 103-02, "Enterprise Architecture Management"
- L. DHS Directive 139-02, "Information Quality"
- M. DHS Instruction 102-01-103, "Systems Engineering Life Cycle Instruction"

IV. Responsibilities

- A. The **DHS Chief Information Officer (CIO)**:
 - 1. Establishes a DHS Enterprise Data Management Office to ensure data management is an integral component of the DHS Enterprise Architecture.
 - 2. Manages the execution of this Directive and Instruction, as administered by the DHS Chief Data Architect, who is the lead for the Enterprise Data Management Office.
 - 3. Ensures the continued operation of an Enterprise Data Management Office.
- B. The **DHS Enterprise Data Management Office (EDMO)**:
 - 1. Develops the DHS strategy for technical management of the sum of all data collected, created, used, managed, maintained, shared and stored by DHS and its Components ("enterprise data management"), and facilitates data management initiatives set forth in the strategy. Data originating from outside of DHS is governed by the enterprise data management strategy if subsequently consumed by a DHS system or service.
 - 2. Provides the authoritative source for enterprise data architecture guidance and governance processes as a basis for the Enterprise Architecture and DHS Information Sharing Environment as outlined in the Federal Enterprise Architecture guidance.

C. The **Component Chief Information Officers:**

1. Ensure Component compliance with DHS Enterprise Architecture, Systems Engineering Life Cycle (SELC), and enterprise data management policies and enterprise data standards.
2. Support Enterprise Architecture and SELC guidance for developing and managing systems and data to assist Component programs in applying best practices and management principles in a consistent manner.

D. The **Executive Director, Information Sharing Environment Office:**

1. Leads and represents DHS in the DHS Information Sharing Environment (ISE).
2. Establishes and maintains the Information Sharing Segment Architecture to align and monitor the development of information sharing capabilities and processes critical to the DHS ISE.
3. Exercises executive leadership in promoting DHS standards, directives, initiatives, and practices with respect to data management and information sharing of enterprise data within the DHS ISE.
4. Ensures information to be shared in the DHS ISE is appropriately tagged with access control, security, privacy, quality, provenance, and descriptive metadata to enable information consumers to appropriately handle and dispose of data they receive.

E. The **Chief Privacy Officer:**

1. Coordinates with the Chief Information Officer and Chief Information Security Officer to provide guidance regarding information technology and technology-related programs and to develop and implement policies and procedures to safeguard personally identifiable information used or maintained by the Department in accordance with federal law and policy.
2. Ensures all DHS interagency and international information sharing agreements comply with DHS privacy compliance documentation requirements and DHS privacy policy.

V. Policy and Requirements

Enterprise Data:

- A. Is to be treated as an asset and handled accordingly. Treating data as an asset means that it is catalogued and safeguarded so it can be made visible, accessible and shareable across DHS and can be made understandable through the use of metadata and other data definition methods.
- B. Is an essential enabler of the DHS ISE and visible, accessible and understandable to authorized users to support mission objectives. Enterprise data is created and maintained as close to the source as feasible to ensure data is authoritative, trusted and meets mission reliability standards.
- C. Includes, but is not limited to, data shared within DHS, data shared with other government agencies and external partners, and data shared within and outside of DHS in the DHS ISE. Exposing shared data available internally or externally through services or application interfaces includes making the information sharing and access agreements and information exchanges of such data visible and accessible.
- D. Includes all related information sharing and access agreements and information exchanges, and is accessible to users who have an authorized purpose and permission within DHS and its Components except where limited by law, regulation, or policy (including but not limited to those applicable to personally identifiable information or protected critical infrastructure information or proprietary trade information), according to the terms of the information sharing access agreement, or by security classification.
- E. Is accessible outside of DHS by providing the data to the DHS ISE and by receiving authorization from the Information Sharing and Safeguarding Governance Board (ISSGB) or from its authorized subordinate bodies such as the Information Sharing Coordination Council (ISCC), Information Safeguarding and Risk Management Council (ISRMC) or other appropriate data governance boards.
- F. Is modeled, named and defined consistently across and within all DHS mission areas, consistent with applicable law and policy. Absent any legal or policy prohibitions, every effort is made to share data across the DHS mission areas and not to maintain redundant data without justification.

G. Has a standard set of metadata including but not limited to associated information assurance and quality, security and access control, privacy sensitivity, records classification/retention/disposition controls, and an authoritative source for the data, which is identified at the lowest level possible, wherever appropriate in the Enterprise Architecture Information Repository.

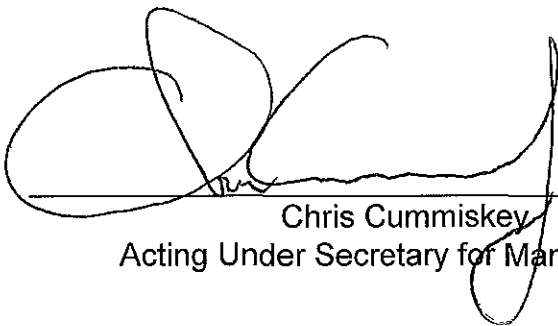
H. Is managed to ensure that data stewards apply the standards of data governance and data quality, consistent with guidance provided by DHS advisory and oversight offices such as the Office of the General Counsel, the DHS Chief Information Officer, and the Office for Civil Rights and Civil Liberties. Compliance with the data governance and data quality standards is provided through the Homeland Security Enterprise Architecture governance process.

I. Is controlled and safeguarded by designated data stewards and oversight offices based on recorded and approved requirements and compliance guidelines.

J. Is developed to be disseminated or shared with the public in a consumable, machine-readable format, wherever possible unless prohibited by safeguards such as those designed to protect classification, the inclusion of personally identifiable information (PII), protected critical infrastructure information (PCII), or trade secret sensitivity.

VI. Questions

Address any questions or concerns regarding this Directive to the Enterprise Data Management Office in the DHS Office of the Chief Information Officer in the Enterprise Business Management Office.


Chris Cummiskey
Acting Under Secretary for Management

8/25/14

Date