U.S. Department of Homeland Security
Washington, DC 20528

PRIVACY POLICY GUIDANCE MEMORANDUM

June 30, 2011

Memorandum Number: 2011-02

MEMORANDUM FOR: DHS Directorate and Component Leadership

FROM: Mary Ellen Callahan
Chief Privacy and Freedom of Information Act Officer

David Heyman
Assistant Secretary for Policy

Richard A. Spires
Chief Information Officer

Karl Johnson
Director of Records, Publications, and Mail Management

SUBJECT: Roles & Responsibilities for Shared IT Services

PURPOSE

This policy establishes a formal Department-wide approach to the roles and responsibilities accompanying cross-component sharing of IT services.

BACKGROUND

Historically, Department of Homeland Security (DHS) Components built individual systems to support individual missions and collected and used data through only those systems to support their unique missions. This "unique mission" model created numerous segmented and segregated implementations of technology, data architectures, and rules for data retention.

This policy establishes the foundation for the change to a service oriented technology architecture and a Shared IT Service and enterprise data environment. This policy sets the responsibilities of the three foundational roles in a Shared IT Services environment: (1) The DHS Component Data Steward; (2) The DHS Component Service Provider; and (3) The DHS Component Data User.

This policy does not cover Component code sharing where code for one system is provided to another Component for the creation of a similar system.

The below sections detail the specific terms, policies, roles and responsibilities that will enable DHS to attain the efficiencies of Shared IT Services and maintain the same level of robust governance of locally operated IT systems and data.

DEFINITIONS

1. Component Data Steward is the DHS Component responsible for ensuring the data is used appropriately throughout the entire data lifecycle. The Component Data Steward is the DHS Component that first identified the business need to collect the data within DHS.

2. Component Service Provider is the DHS Component authorized to provide particular IT service to other DHS Components including the storage, processing, and accessibility of data.

3. Component Data User is the DHS Component that uses data through a Shared IT Service.

4. Shared IT Service is any IT system/technology made available by a DHS Component Service Provider to other DHS Components or external entity.

POLICY

1. DHS fosters reusable IT services and enterprise data to support Component needs in order to improve the quality, consistency, efficiency, and effectiveness of technology and data use throughout the Department.

2. All Shared IT Services shall be published in the Enterprise Architecture Information Repository (EAIR) and approved via the Service Insertion Process (SIP); and only Shared IT Services approved through the SIP and listed in the EAIR may be used.

3. Components could hold multiple roles concurrently. A single Component could be designated as a Component Service Provider, a Component Data Steward, and a Component Data User at the same time.

    a. Components shall meet the requirements of a Component Data User prior to accessing data through Shared IT Services.

    b. All Component Data Stewards will also be considered Component Data Users for the data they steward and shall meet the requirements of the Component Data User role in order to access data through a Shared IT Service.

4. All data used in Shared IT Services shall be published in the DHS Data Asset Repository and only data published in the DHS Data Asset Repository will be used through Shared IT Services.

    a. All uses of data through Shared IT Services shall be compatible with the purpose for which that data was originally collected by DHS.

    b. Some data sets may be the result of contributions from multiple Components. A single Component shall be identified as the Component Data Steward for each logical portion of these blended data sets.

5. All uses of data and Shared IT Services shall comply with all applicable privacy compliance requirements, including all data retention and use limitation requirements.

ROLES & RESPONSIBILITIES

These roles define the scope of responsibilities of DHS Components using Shared IT Services.

1. The DHS Component Data Steward shall:

    a. Document the legal authority and the purpose for the collection and use of the data.

    b. Document criteria for the appropriate use of data through the Shared IT Service.

    c. Document that the Shared IT Service includes sufficient controls to enable the Component Data Steward to validate the use of the data, including managed access.

    d. Ensure that all additional uses of the data are legally authorized, appropriate, and compatible with the purpose for which the data was originally collected.

    e. Ensure and document that the data is maintained according to DHS and National Archives and Records Administration (NARA) approved records retention schedule. If a records retention schedule is not yet approved, ensure that all data is maintained until a records retention schedule is approved. This is the Component Data Steward's responsibility even if another Component physically stores and manages the data.

    f. Complete all privacy compliance requirements for the data including a System of Records Notice.

    g. Publish the data in the DHS Data Asset Repository.

    h. Ensure that all Component Data Users complete all privacy compliance requirements prior to using the data through the Shared IT Service.

    i. Approve and document Component Data Users' use of the data through the Shared IT Service.

    j. Prior to using the data, fulfill all the responsibilities of the Component Data User.

2. The DHS Component Service Provider shall:

    a. Develop the Shared IT Service with capability to control access of data with sufficient granularity to empower the Component Data Steward to validate the use of the data through the Shared IT Service.

    b. Develop the Shared IT Service with audit logging to report on user-data-transactions with sufficient detail to verify compliance with this policy.

    c. Conduct a Privacy Impact Assessment of the service and complete all other privacy compliance requirements prior to making the service available.

    d. Develop the Shared IT Service with capability to maintain independent data retention, disposition, and data access periods for the same data set.

    e. Publish the Shared IT Service in the DHS Services Catalog.

    f. Prior to enabling the Component Data User to access data through the Shared IT Service, confirm that the Component Data Steward authorizes the Component Data User's access of the data through the Shared IT Service.

    g. Prior to accessing the data, meet all the requirements of the Component Data User.

3. The DHS Component Data User shall:

    a. Obtain written approval of the Component Data Steward prior to accessing the data.

    b. Document the authority and purpose for its use of data through the Shared IT Service.

    c. Document criteria for the appropriate use of data through the Shared IT Service.

    d. Complete all privacy compliance requirements related to its use of the Shared IT Service and data prior to using the service.