Department of Homeland Security
DHS Directives System
Directive Number: 103-02
Revision Number: 00
Issue Date: 6/19/2014

ENTERPRISE ARCHITECTURE MANAGEMENT

I. Purpose

This Directive establishes the Department of Homeland Security (DHS) policy on Enterprise Architecture (EA) and defines related roles and responsibilities for ensuring compliance with legislative and executive level guidance on EA.

II. Scope

A. This Directive applies throughout DHS, unless exempted by statutory authority.

B. This cancels and supersedes the Addendum E, "Enterprise Architecture Management," within Management Directive 0007.1, "Information Technology Integration and Management."

III. Authorities

A. Public Law 104-106, Sections D and E, "Clinger-Cohen Act of 1996"

B. Public Law 107-347, "E-Government Act of 2002"

C. Public Law 111-352, "The Government Performance and Results Modernization Act of 2010"

D. Title 44, United States Code, Chapter 35, "Coordination of Federal Information Policy"

E. Office of Management and Budget (OMB) Circular A-11, "Preparing, Submitting and Executing the Budget"

F. OMB Circular A-130, "Management of Federal Information Resources"

G. OMB Memorandum M-13-13, "Open Data Policy – Managing Information as an Asset"

H. DHS Delegation 04000, "Delegation for Information Technology"

IV. Responsibilities

A. The ***DHS Chief Information Officer (CIO)***:

1. Establishes the DHS Enterprise Architecture Program Management Office (EAPMO);

2. Appoints the Enterprise Architecture Director, who also serves as the DHS Chief Architect;

3. Collaborates with stakeholders across the DHS enterprise to identify strategic improvement opportunities, define target architectures, establish EA transition plans, and monitor the implementation of EA transition plans;

4. Ensures that the Enterprise Architecture program complies with applicable laws, OMB, and DHS policies and procedures, and has an effective governance process;

5. Issues procedures/instructions concerning the ongoing development, maintenance, and maturity of the DHS Enterprise Architecture in accordance with OMB and Government Accountability Office directives, instructions, policies, and memoranda of EA;

6. Promotes the practice of EA by establishing and delivering DHS-wide training programs on EA;

7. Ensures that EA practices, principles, and information are incorporated into IT governance, portfolio management, capital planning, investment management, and other processes related to the planning, acquisition, and maintenance of information technology (IT);

8. Establishes annual performance goals for each Component's Enterprise Architecture as well as the overall DHS EA, measures the performance of each the Component's Enterprise Architecture program and overall DHS EA, and provides guidance on methods for continuous improvement;

9. Establishes the Enterprise Architecture Center of Excellence (EA COE) to promote and support the planning, implementation, and maturing of EA across DHS. The EA COE is a collaborative body that is chaired by the DHS Chief Architect and comprises the Chief Architects from each Component along with appropriate specialists from other DHS offices; and

10. Ensures that DHS Data Management practices and principles are incorporated into Component's data management, information sharing and EA efforts and measures the performance of each Component's data management and information sharing effort on the Enterprise Data Management Scorecard.

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

1. Appoint and designate the Component Chief Architect (Chief Technology Officer or other like official) and provide resources for the execution of an EA Program;

2. Communicate Departmental EA policies, processes, and procedures throughout the Component and ensure all Component employees and contractors are in compliance;

3. Support the development and implementation of target architectures and transition plans across the segments of the DHS EA in collaboration with mission stakeholders and the DHS CIO or EAPMO;

4. Certify the sufficiency and completeness of Component information in DHS EA annually prior to the submission of the Homeland Security Architecture to OMB;

5. Provide periodic updates to the essential Component-related information at the appropriate level of detail in the DHS EA and in accordance with guidance from the DHS CIO or EAPMO;

6. Monitor the status of all conditions levied by the DHS EA Board on IT programs/projects, ensuring that conditions are resolved in a timely manner, and provide a monthly report to the DHS CIO on the status of any unresolved conditions;

7. Promote the practice of EA by establishing and delivering DHS-wide training programs on EA within their respective Component and actively participating in the EA COE; and

8. Ensure that EA practices, principles, and information are incorporated into IT governance, portfolio management, capital planning, investment management, and other processes related to the planning, acquisition, and maintenance of information technology.

V. Policy and Requirements

A. The DHS EA Program provides a vehicle to tie the strategic mission goals and objectives of DHS to the business processes, information resources and technology investments necessary to reach key performance outcomes. The EA provides a resource of information about the performance metrics, lines of business, information and the enabling services and technologies currently used within DHS. The EA also provides the roadmap for implementing the capabilities needed to achieve the Department's key performance outcomes and ensures efficient use of resources.

B. The DHS EA complies with legislative mandates, Federal initiatives, and oversight requirements. Specifically, the Federal Enterprise Architecture is used as guidance.

C. All DHS IT systems aligns with the Department's EA.

D. Employees and officials implements the EA consistent with the following principles:

1. Develop information systems and services that facilitate interoperability and sharing of applications across DHS;

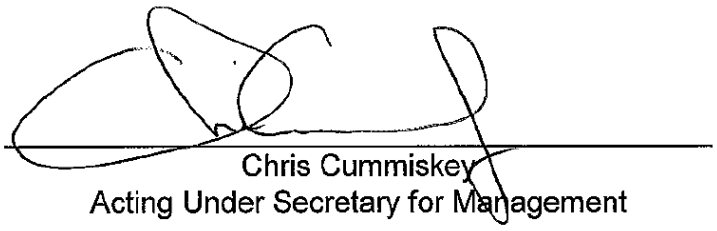
2. Meet information technology needs through cost effective intra-agency and interagency sharing and reuse of existing capabilities, before acquiring new IT resources;

3. Establish a level of security for all information systems that is commensurate to the risk and magnitude of the harm resulting from the loss, misuse, unauthorized access to, or modification of the information stored in or flowing through these systems; and

4. Develop information systems that utilize cost-effective data management and data architecture practices to ensure data is trusted, reliable, and reusable.

VI. Questions

Address any questions or concerns regarding this Directive to the Office of the Chief Information Officer.



Chris Cummiskey
Acting Under Secretary for Management

6/12/14
Date