Department of Homeland Security
DHS Directives System
Directive Number: 262-09
Revision Number: 00
Issue Date: 05/30/2017

ENTERPRISE INFORMATION TECHNOLOGY SERVICE MANAGEMENT

I. Purpose

A. This Directive establishes the Department of Homeland Security (DHS) Enterprise Information Technology (IT) Service Management policy.

B. Enterprise IT Services are a collection of mission support tools, applications, and IT infrastructure that support or enable mission capabilities across the DHS enterprise that enable common capabilities at an affordable cost and within defined service level agreements; and available for consumption by one or more Components and are typically delivered through internally or externally cloud-based or legacy infrastructures.

II. Scope

This Directive applies throughout DHS, regarding Enterprise IT Services, with the exception of the Office of Inspector General.

III. Authorities

A. Public Law 113-291, "Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015," Title VIII, "Acquisition Policy, Acquisition Management, and Related Matters," Subtitle D, "Federal Information Technology Acquisition Reform"

B. Title 44, United States Code (U.S.C.), Chapter 35, "Coordination of Federal Information Policy" and Chapter 36, "Management and Promotion of Electronic Government Services"

C. Office of the Management and Budget (OMB) Memorandum M-11-29, "Chief Information Officer Authorities" and OMB Memorandum M-12-10, "Implementing PortfolioStat"

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

E. DHS Directive 142-02, "Information Technology Integration and Management" and its implementing Instruction

F. National Institute of Standards and Technology (NIST), "The NIST Definition of Cloud Computing," Special Publication 800-145 and "Cloud Computing Synopsis and Recommendations," Special Publication 800-146

G. DHS Directive 140-01, "Information Technology Systems Security"

H. DHS Directive 102-01, “Acquisition Management” and its implementing Instructions

I. DHS Directive 107-01, “Joint Requirements Integration and Management System” and its implementing Instruction

IV. Responsibilities

A. The ***Under Secretary for Management (USM) as the DHS Chief Acquisition Officer (CAO)***: As designated by Title 41 U.S.C, Section 1702(b), is responsible for DHS acquisitions. The CAO responsibilities are delineated in DHS Directive 102-01 and its implementing Instructions. The CAO chairs the Acquisition Review Board (ARB) that reviews all major (level 1 and level 2) acquisitions – including IT Services - at the Acquisition Decision Events (ADEs) in the Acquisition Lifecycle Framework (ALF). The DHS Chief Information Officer (CIO) reports to the USM who has overall leadership for the Department’s mission support systems and delegates IT responsibilities to the DHS CIO.

B. The ***DHS CIO***:

1. Provides leadership for the strategy, design, development, security, implementation, enhancement, and maintenance of DHS Enterprise IT Services;

2. Promotes the use of Enterprise IT Services for mission and support functions across multiple Components;

3. Develops Enterprise IT Services requirements and makes service investment decisions based on documented end user requirements and approved Enterprise IT Services policies and processes;

4. Develops and implements the methodology for managing IT services and integrating Enterprise IT Services and investments into the OMB Capital Planning and Investment Management evaluation and reporting system for the Department; and

5. Governs and maintains a Service Management Framework for Enterprise IT Services.

C. The ***Component Heads***:

1. Use Enterprise IT Services as outlined in this Directive, through the Component CIOs; and

2. Ensure Enterprise IT Services are adequately supporting the desired mission objectives within their Components.

D. The ***Component CIOs***:

1. Provide requirements and support design and testing of Enterprise Services;

2. Implement policies and procedures necessary to ensure compliance with this Directive;

3. When seeking to add new IT capabilities, leverage existing Enterprise IT Services before establishing new capabilities when appropriate through;

a. Reviewing new and existing Enterprise IT Services to determine their suitability for the Component's mission. If an Enterprise IT Service meets the mission requirements, support business case development, and transition planning;

b. Overseeing the implementation of the Component's use of Enterprise IT Services; and

c. Identifying Component IT Services that could be consumed across the Enterprise and reporting those services to the Deputy CIO Council (DCIO Counsel).

4. Gather feedback from users and translate customer needs into capabilities for the Enterprise IT Services;

5. Ensure Enterprise IT Services adequately account for organizational information security needs; and

6. Ensure Enterprise IT Services are meeting their intended and desired outcomes within their Components.

E. The ***Chief Information Officer Council***:

1. With consent of the USM, the CAO approves all new Enterprise IT Services prior to release into a production environment;

2. Promotes the strategic vision for Enterprise IT Services; and

3. Promotes the use and implementation of Enterprise IT Services.

F. The ***DCIO Council***:

1. Supports the strategic vision of the CIO Council through program execution;

2. Serves as an advisory board to the CIO Council, recommends and oversees new and ongoing Enterprise IT Services efforts;

3. Ensures the Program Office will coordinate with the DHS Privacy Officer, Records Officer, and other cognizant accountability officials and programs to ensure regulatory compliance requirements are identified and proactively addressed within new and ongoing Enterprise IT Services efforts;

4. Sponsors Enterprise IT Service projects across the Department and encourages participation from various organizations; and

5. Ensures Enterprise IT Services are included in the DHS IT Services Catalog.

G. The ***Executive Steering Committee (ESC)***: Provides guidance and support to acquisitions between ADEs and provides technical direction and support in accordance with the Acquisition Decision Authority approved ESC charter.

H. The ***Enterprise IT Services Board***: Enables the CIO's strategy, oversees the Enterprise IT Services portfolio, and develops and maintains the Enterprise IT Services roadmap.

I. The ***Joint Requirements Council***: Provides oversight of the DHS requirements generation process, and harmonizes efforts across the Department. It directs analysis to validate the need and gaps for all acquisitions with respect to requirements.

J. The ***Enterprise Architecture Board***: Ensures the proposed enterprise IT solutions are consistent with the enterprise technical architecture.

K. The ***Infrastructure Change Control Board***: Ensures that changes to DHS enterprise unclassified IT infrastructure are planned, engineered, tested, coordinated, and approved prior to their implementation.

L. The ***Chief Privacy Officer:***

1. Ensures that the Department's use of technology sustains, and does not erode, privacy protections relating to the collection, use, maintenance, disclosure, deletion, and destruction of Personally Identifiable Information;

2. Evaluates Enterprise IT Services proposals for privacy impacts and provides guidance to safeguard personally identifiable information in accordance with federal law and policy; and

3. Reviews and approves all Department Privacy Compliance documentation.

M. The ***Chief Financial Officer:***

1. Provides existing costs of legacy IT service that could be replaced by an Enterprise IT service;

2. Provides cost modeling for a Component hosted service that could become an enterprise service; and

3. Ensures proper budget is allocated to pay for an enterprise service including funds to retire the legacy service, when appropriate.

V. Policy and Requirements

It is DHS policy that:

A. The CIO Council, consent of the USM/CAO, approves all Enterprise IT Services before such services go into production environment.

B. All DHS Components:

1. Review Enterprise IT Services to determine whether such services can meet Component mission needs.

2. Consolidate IT Services into the Enterprise IT Service environment to reduce duplication of products and services. If Enterprise IT Services cannot be used, provide analysis explaining the reason it cannot be used in place of a legacy application and/or infrastructure for technical reasons or for budgetary reasons. This is in accordance with 15 U.S.C. 644(e) and the Federal Acquisition Regulation (FAR) 7.107.

3. Provide insight into the business processes, technical specifications, financial commitments, and other feedback on Enterprise IT Services.

4. Comply with the IT Services Lifecycle and the ALF.

C. ***IT Services Lifecycle (ITSLC)***:

1. The ITSLC represents the standardized implementation approach for Enterprise IT Service Management and is a tailored path of the Systems Engineering Life Cycle. It integrates five supporting business processes: Plan, Design, Deploy, Operate, and Implement performance measures. The ITSLC defines the governance for three categories of services: Enterprise IT, Mission/Business, and Data.

2. Acquisitions for Enterprise IT Services fully comply with the ALF and Systems Engineering Life Cycle established by DHS Directive 102-01.

VI. Questions

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

Chip Fulghum
Acting Under Secretary for Management

5/30/17
Date