

INFORMATION TECHNOLOGY INTEGRATION AND MANAGEMENT

I. Purpose

This Directive establishes the responsibilities and policies of the Department of Homeland Security's (DHS) Chief Information Officer (CIO) and DHS Component Chief Information Officers (Component CIOs) regarding information technology (IT) integration and management.

II. Scope

This Directive applies throughout DHS. Nothing in this Directive impedes the statutory authority of the United States Secret Service.

III. Authorities

- A. Clinger-Cohen Act of 1996, Title 44, United States Code (U.S.C.) §§ 11101-11704
- B. Federal Information Security Modernization Act of 2014 (FISMA), 44 U.S.C. §§ 3551-3558
- C. 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" as codified in relevant part at 40 U.S.C. § 11319 (FITARA)
- D. Title 6, U.S.C. § 341, "Under Secretary for Management" and §343, "Chief Information Officer"
- E. Federal Acquisition Regulation, Part 39, "Acquisition of Information Technology"
- F. Office of Management and Budget (OMB) Circular A-130, "Managing Information as a Strategic Resource"
- G. OMB Memorandum M-15-14, "Management and Oversight of Federal Information Technology"
- H. Delegation 00002, "Delegation to the Under Secretary for Management"

- I. Delegation 00500, “Delegation for Administrative Services”
- J. Delegation 00702, “Delegation to the Chief Procurement Officer”
- K. Delegation 01000, “Delegation for Financial Activities”
- L. Delegation 03000, “Delegation for Human Capital and Human Resources”
- M. Delegation 04000, “Delegation for Information Technology”
- N. Delegation 13001, “Delegation to the Chief Privacy Officer”

IV. Responsibilities

A. The **Under Secretary for Management (Chief Acquisition Officer)**:

1. Serves as the DHS official through which all Department-wide IT activities and services are acquired, overseen, defined, and measured; and
2. Ensures IT is managed consistently with all statutory, regulatory, and Departmental requirements and in alignment with the strategic plans of the Department.

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

1. Fulfills all responsibilities of the Department’s Chief Information Officer as specified by applicable statutory provisions and policy direction;
2. Establishes the IT strategy, policies, and business processes necessary to align IT activities across the Department;
3. Improves efficiency, effectiveness, and accountability in all aspects of IT acquisition and operations by providing management, governance, oversight, and direction to all Components and headquarters elements. Collaborates as a full partner with the Management Directorate (MGMT) Lines of Businesses with respect to IT;
4. Implements an Information Security Program in accordance with the Federal Information Security Modernization Act of 2014, Executive Order 13800 “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,” and Directive 140-01, “Information Technology Security Program”;
5. Establishes the plan for the ongoing recapitalization of IT resources across the Department;

6. Establishes and oversees the Capital Planning and Investment Control process within the Department;
7. Establishes and manages the IT Acquisition Review (ITAR) process to review and approve acquisitions that contain IT and approve the acquisition plans, requirements documents, cost estimates and such other documents associated with the related contracts as required by FITARA and the Homeland Security Acquisition Manual Chapter 3039.170, and such other procurements and acquisitions as the CIO deems necessary, with such delegations as the CIO deems appropriate and are allowed by law;
8. Ensures that IT Investments are aligned with Department and Component strategy and missions and conducts annual IT portfolio reviews and participates in the OMB PortfolioStat process to evaluate and prioritize IT investments, identify duplication and waste, develop opportunities for consolidation and shared services, and identify opportunities for savings in purchases of commodity IT and IT infrastructure through category management and enterprise strategic sourcing;
9. Evaluates IT investments, programs, and systems to ensure ongoing alignment with mission needs, increase efficiency and effectiveness, evaluate and assign risk, and promote use of incremental development methodologies;
10. Reviews high-risk IT investments to determine root causes, develop corrective actions, evaluate ongoing performance, and recommend executive action to continue, reassess, or terminate the investment;
11. In conjunction with the DHS Chief Financial Officer, coordinates and approves DHS IT budget requests and budget execution plans for all IT resources (see [Directive 101-01](#) and [Instruction 101-01-001](#));
12. Establishes, chairs, or participates on governance boards that include IT resources, including the DHS Acquisition Review Board and the Joint Requirements Council;
13. Develops and maintains, with the Chief Human Capital Officer (CHCO) and Chief Procurement Officer, a current workforce planning process for IT staff across the Department, including establishing IT competency requirements;
14. The CIO participates in the hiring and selection processes for Component CIOs. In collaboration with the relevant Component Head, and except as otherwise provided by law, the CIO provides concurrence on the DHS-wide selection and hiring of Component CIOs and Deputy CIOs throughout DHS. Additionally, consistent with applicable Department Executive Resources processes, Components submit selection actions, documenting the CIO concurrence, through the Office of the Chief Human Capital Officer (OCHCO) and Under Secretary for Management for approval by the Deputy Secretary.

- a. For hiring and selection activities, Components:
 - (1) Submit job opportunity announcements for the Component CIO position, documenting the CIO concurrence, through OCHCO and the Under Secretary for Management for approval by the Deputy Secretary.
 - (2) Invite the CIO or their designee to participate in the interview process of the best qualified list of candidates; and
 - (3) Secure CIO concurrence through OCHCO and the Under Secretary for Management for approval by the Deputy Secretary prior to extending a job offer.
- b. For performance evaluations, Components:
 - (1) Submit proposed performance objectives and standards and performance plans for consideration to the CIO prior to finalization with the affected employee;
 - (2) Secure CIO concurrence with proposed performance evaluations and appraisals, bonus or award recommendations, pay adjustments, and/or other forms of commendation prior to issuance; and
 - (3) Confer with the CIO to resolve any substantive performance issues.

15. Establishes and manages the DHS enterprise architecture and data management framework;

16. In conjunction with the Under Secretary for Intelligence and Analysis, develops the information sharing environment throughout the Department;

17. Implements a Digital Services and Geospatial Program;

18. Implements an Accessible Systems and Technology Oversight Program;

19. Ensures that DHS websites, web pages, and web portals adhere to laws, regulations, policies, and guidance regarding IT and network security; and

20. Oversees the Department's compliance of Records Management and Retention, Forms Management, Librarian Services, Printing, Paperwork Reduction Act, and Information Quality Act.

C. The **Component Heads** in accordance with the authorities granted in DHS Delegation 04000, Section II.C:

1. Designate the Component's CIO with approval from the DHS CIO;
2. Obtain the approval of the DHS CIO prior to purchasing any IT Asset (this applies only to Support Component heads, excluding the Federal Law Enforcement Training Center); and
3. Advise and collaborate with the DHS CIO on Component reorganization or restructuring plans concerning IT functions.

D. See [Appendix A](#) for additional responsibilities of the Component Chief Information Officers, DHS Chief Procurement Officer, DHS Chief Financial Officer, DHS Chief Privacy Officer, DHS Chief Human Capital Officer, and DHS Chief Readiness Support Officer.

V. Policy and Requirements

It is the policy of the Department to acquire and manage IT in a manner that:

- A. Ensures that IT systems are aligned with each Component's mission, justified in each strategic and capital planning process, funded by an appropriate IT budget, and managed as investments;
- B. Engages the Chief Information Officer Council, overseeing the implementation of IT across the Department;
- C. Achieves the mission objectives identified by the Department's Strategic Plan and related policies; and
- D. Complies with relevant statutes, regulations, and policies.

VI. Questions

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



Claire M. Grady
Under Secretary for Management

12 APR 2018

Date

Appendix A: Additional Responsibilities

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

1. Provide timely delivery of mission IT in direct support of the mission, goals, objectives, and programs of the Component;
2. Comply with all Departmental IT policies, processes, standards, guidelines, and procedures;
3. Implement the requirements of all applicable statutory provisions, including Clinger-Cohen and the Federal Information Technology Acquisition Reform Act (FITARA), in conjunction with the DHS CIO and other Management Directorate Lines of Business Chiefs; appoint a FITARA point of contact to coordinate FITARA implementation with the FITARA lead for DHS;
4. Ensure that IT Investments are aligned with Department and Component strategy and missions; conduct annual IT portfolio reviews to evaluate and prioritize IT investments, identify duplication and waste, and develop opportunities for consolidation and shared services;
5. Coordinate the ongoing recapitalization of IT resources with the Department;
6. Evaluate IT investments, programs, and systems to ensure ongoing alignment with mission needs, increase efficiency and effectiveness, evaluate and assign risk, and promote use of incremental development methodologies;
7. Review high-risk IT investments to determine root causes, develop corrective actions, evaluate ongoing performance; and recommend executive action to continue, reassess, or terminate the investment;
8. In conjunction with the Component Senior Financial Officer, develop, review, and approve the Component IT budget and spend plans, including any transfer or reprogramming of funds for IT resources;
9. Establish and manage the Component IT Acquisition Review (ITAR) process;

Appendix A: Additional Responsibilities

10. Review and approve acquisitions that contain IT and approve the acquisition plans, requirement documents, cost estimates and such other documents associated with the related contracts as required by FITARA and the Homeland Security Acquisition Manual Chapter 3039.170, and such other procurements and acquisitions as the Component CIO deems necessary, with such delegations to other OCIO executives as the Component CIO deems appropriate and are allowed by law. Appoint one or more coordinators to manage the Component ITAR process and liaise with the DHS ITAR process;
11. In conjunction with the Component Acquisition Executive, participate as a decision maker in the Component Acquisition Review process with respect to IT acquisitions;
12. Participate on all Component governance bodies that oversee IT resources and on the Chief Information Officer Council, Enterprise Architecture Board, and other council/boards as appropriate;
13. Communicate with and educate the Component Heads, Councils, and Component leadership teams across all lines of business regarding the DHS CIO Council priorities and initiatives;
14. In alignment with DHS strategy and policy, develop, implement, and maintain a detailed IT strategic plan and enterprise architecture, maintain programs for Accessible Systems and Technology oversight, Enterprise Data Management, and Information Security; and
15. Meet the IT competency requirements established by the DHS CIO, as required in the Component CIO's performance plan.

B. The **DHS Chief Procurement Officer**.

1. Issues policy requiring that procurement request packages including IT contain documentation of approval for the procurement by the DHS CIO, Component CIO, or designee as required by FITARA prior to processing by the contracting activity; and
2. Provides data to the DHS CIO or designee on IT Program Manager Certification level (Federal Acquisition Certifications).

Appendix A: Additional Responsibilities

C. The **DHS Chief Financial Officer (CFO)**:

1. Conducts the annual Program and Budget Review (PBR), justifies the budget to OMB and Congress, oversees the execution of current and prior-year budgets, and assesses progress towards Department-wide performance goals. As part of the PBR and the FYHSP development, the CFO presents the substantive, large-scale alternatives to the appropriate governance body;
2. In conjunction with the CIO, the CFO exercises a significant role in the decision processes for the annual and multi-year planning, programming, budgeting and execution decisions for programs that include IT resources, and recommends approval of budget requests for IT resources;
3. The CFO and CIO jointly affirm and certify that the CIO has reviewed and approved the major IT investments portion of the budget request, and that the CIO has a significant role in reviewing planned IT support for major program objectives and significant increases and decreases in IT resources; and
4. In conjunction with the CIO, the CFO maintains the CFO Designated Systems List, which includes those systems that process, accumulate, and/or maintain financial data for the Department. These systems are subject to additional security control requirements based on Office of Management and Budget (OMB) Circular A-123, Management's Responsibility for Internal Control, Appendix A.

D. The **DHS Chief Privacy Officer**:

1. Reviews IT capital investment plans and budgetary requests to ensure that privacy requirements (and associated privacy controls), as well as any associated costs, are explicitly identified and included with respect to any IT resources that will be used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information (PII).
2. Reviews and approves the privacy plans for agency information systems prior to authorization, reauthorization, or ongoing authorization and reviews authorization packages for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII to ensure that privacy risks are managed prior to system authorization.

Appendix A: Additional Responsibilities

3. Conducts and documents the results of privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency across all agency risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks.
4. Coordinates with CIO and other DHS and Component officials in the implementation of privacy requirements as OMB may establish.

E. The **DHS Chief Human Capital Officer:**

1. Manages the recruiting process for Component Chief Information Officer and ensures the CIO role in the selection and performance management process;
2. Works with the CIO and Chief Procurement Officer to develop training, career paths, competency standards, and innovative means of attracting and retaining information technology acquisition and program management personnel.

F. The **DHS Chief Readiness Support Officer** establishes the Asset Management Program and works with the DHS CIO on the management of IT Assets.