Department of Homeland Security
Management Directives System
MD Number: 0007.1
Issue Date: 03/15/2007

INFORMATION TECHNOLOGY INTEGRATION AND MANAGEMENT

I. Purpose

A. This Management Directive (MD) establishes the Department of Homeland Security's (DHS) vision and the authorities and responsibilities of the Department's Chief Information Officer. It reinforces the commitment to create and manage a unified Department in mission accomplishment and support systems performance. This MD is the principal document for leading, governing, integrating and managing the Information Technology (IT) function throughout DHS. Essential to the success of the Department's operations is an integrated, support infrastructure designed to function in a highly dynamic environment. The Strategic Goal of unifying the Department mandates a collaborative approach from every entity within the Department.

B. Creating functional excellence requires every executive, manager and employee in the Department to create an environment that rewards collaboration, promotes best practices and shares accountability for the performance of the management support systems that enable the Department to fulfill its mission. This concept of dual accountability mandates that both Component heads and key departmental functional experts are responsible for organizational excellence. The Line of Business Chiefs described herein will be held accountable for designing the system to optimize the IT function, setting the standards for functional performance, creating the department-wide policies and processes, providing the automated solutions to yield greater efficiencies and nurturing the development and success of centers of excellence. Component heads will likewise be accountable to support these progressive business functions as a key part of their commitment to mission accomplishment.

C. In all efforts of this magnitude the integration and alignment of each function requires strong communication, respect for both individuals and process, and a shared resolve to find solutions that benefit both mission accomplishment and functional excellence. DHS leadership across the Department must challenge traditional approaches, communicate, and execute as a team to design and execute these support functions that will constitute progressive 21st century excellence in governance.

II. Scope

This MD applies to all DHS Components, unless exempted by statutory authority.

III. Authorities

A. Public Law 104-106, Divisions D and E, (as amended), "Clinger-Cohen Act of 1996" (previously, "Information Technology Management Reform Act;" renamed by Public Law 104-208)

B. Public Law 107-296, (as amended) "Homeland Security Act of 2002"

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

D. 44 U.S.C. 3506, "Federal agency responsibilities"

E. Federal Acquisition Regulation Part 39, "Acquisition of Information Technology"

F. Homeland Security Acquisition Regulations

G. Office of Management and Budget (OMB) Circular A-130, "Transmittal Memorandum #4, Management of Federal Information Resources"

H. DHS Management Directive 8200.1, "Information Quality"

I. Delegation 0201.1, "Delegation to the Under Secretary for Management"

IV. Definitions

A. ***Business model***: Identifies, defines and documents the functions performed by a Component or by DHS as a Department, identifies organizational units that perform each function, the information (data) used to perform a function; when a function is performed, where a function is performed; and how often a function is performed. The business model is documented in the DHS Enterprise Architecture as part of the Business Reference Model and as defined by the Federal Enterprise Architecture Framework released by the Office of Management and Budget.

B. ***Center of excellence***: An organizational entity with expertise, capabilities and resources in a specific discipline area chartered to support DHS-wide requirements. The mission, charter, roles, responsibilities, resources, authority, implementation plans and service level agreements for each enterprise level IT center will be reviewed by the DHS Chief Information Officer Council and approved by the DHS Chief Information Officer.

C. ***Component***: All the entities that report directly to the Office of the Secretary, the Secretary, Deputy Secretary and his or her staff, Chief of Staff and his or her staff, and Counselors and their staff. See DHS Management Directive 0010.2.

D. ***Component Chief Information Officer***: The Component Chief Information Officer, appointed by the Component head, is the senior-most federal executive in the Component exercising leadership and authority over mission-unique IT policies, programs, services, solutions, and resources. The Component Chief Information Officer acts to implement the policies of the DHS Chief Information Officer. The Component Chief Information Officer has the authority to execute this MD. This authority includes the unilateral authority to determine IT investments.

E. ***DHS Chief Information Officer***: The Department's Chief Information Officer, is the line of business (LOB) chief that exercises leadership and authority over IT policy and programs DHS-wide.

F. ***Chief Information Officer Council***: The IT functional advisory body that assists the DHS Chief Information Officer in evaluating and determining the best course of action for the IT Function. The Chief Information Officer Council is chaired by the DHS Chief Information Officer.

G. ***Dual accountability***: The shared responsibility of both Component heads and line of business chiefs to build a progressive 21st century DHS. Dual accountability recognizes mission accomplishment as the ultimate responsibility of the Component heads and also requires them to support functional integration. Dual accountability recognizes the LOB Chiefs' professional expertise in their specialty area and consequently their primary responsibility to drive functional excellence across DHS and to focus on DHS mission accomplishment.

H. ***Enterprise IT services and solutions***: Enterprise IT services or solutions are those IT services and solutions that are tightly aligned with and support Departmental or inter-agency portfolios that may cross Component lines. These programs will be identified by the Department and will be driven by the Departmental recognition that there are compelling reasons to integrate certain Component mission applications, technology solutions, or infrastructure utilities to better deliver Departmental capability and to more effectively marshal resources.

There may also be certain IT services or solutions that will be determined by the Chief Information Officer Council to be enterprise in nature. These may be IT tools, utilities, or services that are predominantly used by the IT function and have not otherwise been identified as enterprise programs by the DHS Investment Review Process.

I. ***Functional integration***: Is a transformation process that enhances efficient and effective use of resources by establishing unified policies and business processes, the use of shared or centralized services and standards and automated solutions. Functional integration is a structured cooperation and collaboration among DHS Components and LOB chiefs for the purpose of achieving functional excellence in support of Departmental mission and objectives. This is accomplished by decreasing fragmentation and duplication, providing enhanced integrated services and increasing efficiency and quality of management lines of business.

J. ***Information technology (IT)***: Any equipment or interconnected system or subsystem of equipment/software, or any national security system, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display (including geospatial technologies), switching, interchange, transmission (wired or wireless telecommunications), or reception of data, voice, video, or information by an executive agency. For purposes of this MD, equipment is used by DHS if the equipment is used by DHS directly or is used by DHS organizational partners (including other federal agencies, state and local governments and private contractors) under a contract with DHS which (a) requires the use of such equipment, or (b) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. It includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources. It does not include any equipment acquired by a contractor incidental to a contract, or equipment which contains imbedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

K. ***Information technology function***: The personnel resources, IT assets, budgets and processes used to deliver mission and Enterprise IT services and solutions.

L. ***Key IT officials***: IT personnel occupying the following positions: Component Chief Information Officer, Component Deputy Chief Information Officer and Senior Enterprise IT Official.

M. ***Line of business (LOB) chiefs***: For the purposes of this MD, the DHS Chief Procurement Officer, Chief Administrative Officer, Chief Financial Officer, Chief Human Capital Officer, Chief Security Officer and Chief Information Officer.

N. ***Mission IT services***: IT services and solutions that are tightly aligned with and directly support a Component mission as defined by law or regulation, the Office of the Secretary or the DHS Component head.

O. ***Office of the Chief Information Officer (CIO)***: The DHS organization that manages and directs the information technology functional area. This office is headed by the DHS Chief Information Officer who is directly supported by CIO staff functions and the Chief Information Officer Council.

P. ***Senior enterprise IT official***: The senior-most Federal IT employee in an enterprise IT service.

Q. ***Service level agreement (SLA)***: Formal agreement that defines customer service expectations and responsibilities between DHS Components and support service providers, whether internal or external. SLAs are defined or renewed annually and are used to communicate baseline mission service requirements. The SLAs will be signed by the responsible official providing the services, the responsible official receiving the services and approved and signed by the DHS Chief Information Officer.

V. Responsibilities

A. The ***Under Secretary for Management*** is responsible for:

1. Providing oversight and management of information and technology systems in DHS, encompassing the general policy direction for all information technology programs within the Department. The Under Secretary ensures the strategic plans of the DHS Chief Information Officer are coordinated with and are mutually supportive of the efforts of the other LOB chiefs. This continuous review by the Under Secretary serves to ensure that supportive and complementary integration between or among functions as well as within the function is identified and completed.

2. Working with the LOB chiefs to design and implement the optimum Department-wide integrated systems to improve mission support. This effort requires a team approach, working in collaboration with all Components, to drive performance excellence in each function in order to create the most progressive support system possible.

B. ***Component heads*** are responsible for:

1. Recognizing their shared, related and inter-dependent responsibility to collaborate and deliver effective and efficient services throughout the Department. In addition, all Component heads must recognize the unique challenges presented by the mission of DHS and plan to ensure the continued delivery of effective services in the event of national emergencies and disasters.

2. Working together to achieve organizational and systems alignment over time such that coherent, analogous organizational structures are built between Components to foster management greater efficiency and clarity.

3. Ensuring that IT management duties, as outlined in this MD, are implemented effectively and efficiently in support of mission accomplishment and functional integration goals.

4. Supporting and implementing the annual goals established in collaboration with the DHS Chief Information Officer.

5. Receiving approval and input from the DHS Chief Information Officer regarding input into performance plans, appraisals, bonus or award recommendations, pay adjustments and other forms of commendation of Component key IT officials. In the spirit of dual-accountability, the Component head and Under Secretary for Management will confer to resolve any issues.

6. Collaborating with the DHS Chief Information Officer in recruiting and selecting Component key IT officials, in the following manner:

   a. Seeking approval of the DHS Chief Information Officer on the qualification standards, including knowledge, skills and abilities or competencies for said position(s);

   b. Seeking the approval of the DHS Chief Information Officer in identifying candidates for consideration;

c. Providing the DHS Chief Information Officer the opportunity to participate in the interview process of the best qualified list of candidates; and

d. Seeking the approval of the DHS Chief Information Officer on final selection.

7. Ensuring the Component Chief Information Officer is organizationally placed at a senior level and is included in the Component's strategic leadership team.

8. Advising and collaborating with the Under Secretary for Management on any Component reorganization or restructuring plans that will result in functional realignments outside of the line of business and any action that would reduce stature or level within the line of business.

9. Ensuring the Component participates in the development and execution of the DHS enterprise architecture.

10. Submitting IT acquisitions and IT budgets to the DHS Chief Information Officer, Chief Financial Officer, and the Chief Procurement Officer for review and approval according to appropriate laws and the policy of the Department.

C. The ***DHS Chief Information Officer*** is responsible for:

1. Conducting program reviews in the IT function and, in turn, recommending program improvements, corrective actions and, if necessary, revocation of delegated authorities for the IT function. This may include the cancellation of an IT acquisition, procurement, or initiative.

2. Advising and assisting the Office of the Secretary, Component heads and other senior officials in carrying out DHS' responsibilities for all activities relating to the programs and operations of the Department's IT function.

3. Communicating and implementing the Secretary's and Under Secretary for Management's leadership direction related to the IT function.

4. Designing, in collaboration with the Chief Information Officer Council, the optimum structure, processes and systems to support both Departmental and Component missions and goals and to achieve IT functional excellence. This includes defining functional performance metrics and the use of SLAs by which the Components can measure the performance of delivered mission IT services and enterprise IT services and solutions.

5. Establishing Department IT priorities, policies, processes, standards, guidelines and procedures.

6. Collaborating with Component heads in recruiting and selecting Component key IT officials, as described in Paragraph V.B.6 herein.

7. Providing the Component Chief Information Officers written performance objectives for the IT function at the start of the performance cycle. The DHS Chief Information Officer will also provide input/feedback to the rating official for the Component Chief Information Officer's and key IT official's accomplishment of those objectives and will approve bonus or award recommendations, pay adjustments and other forms of commendation.

In effect, there will be a "dotted-line" reporting relationship from Component CIO's to the DHS Chief Information Officer.

8. Delegating certain authorities to Component Chief Information Officers, as necessary, to ensure their appropriate and efficient administration and management of Component IT mission services.

9. Providing the Office of the Secretary and Component heads an annual evaluation of IT program performance. This will include an assessment of each Component's functional performance. Reports prepared by the end of the first quarter each fiscal year will include the President's Management Agenda, the DHS Strategic Plan and other program metrics as they are established.

10. Analyzing workforce requirements for functional personnel to establish recommended staffing and resource level parameters and guidelines for each Component to consider.

11. Chairing the Chief Information Officer Council and Enterprise Architecture Board.

12. Overseeing the development of reimbursable agreements for cross-Component delivery of IT services where required.

13. Developing and maintaining a statutorily compliant Information Security Program consistent with the authorities granted in the Federal Information Security Management Act of 2002 (FISMA) (Public Law 107-347, Title 111).

14. In conjunction with the DHS Chief Procurement Officer, coordinating and implementing an acquisition strategy for delivering and maintaining enterprise IT solutions and services. This will include:

IT Acquisitions (in excess of $2.5 Million):

a. Reviewing and approving any IT acquisition in excess of $2.5 million (may be in a Service Level Agreement, Purchase Request, Inter-Agency Agreement, etc.). This value may be any of the following:

(1) full value of the acquisition (e.g., the cumulative value of a multi-year contract);

(2) funding for the fiscal year option of a multi-year contract if it exceeds $2.5 million; or

(3) life cycle of the project (e.g., "document authorizing the acquisition" could be the business case/Office of Management and Budget Form 300 approved by the Investment Review Board).

b. Providing comments and recommendations within ten (10) business days of receiving the documentation.

c. Establishing a method to electronically document the receipt and status of the procurement request.

d. Providing this review process to all the Components via separate correspondence.

For those purchases under $2.5 million, the Component CIO will approve these with in their respective Components, and provide a monthly report of these approvals to the CIO within ten (10) working days from the end of each month.

15. With the support of the Component head and through the Component Chief Information Officers, organizing appropriate IT resources for enterprise IT services and solutions and providing the direction required to achieve DHS' requirements.

16. Establishing training, development and certification guidelines for IT professionals. Achieving certification goals may be met through a multiyear plan submitted by the Component to the Chief Information Officer.

17. In conjunction with the DHS Chief Financial Officer, coordinating and implementing an IT budget strategy for delivering and maintaining enterprise IT solutions and services. This will include:

IT Budget:

a. Submitting to the DHS Chief Financial Officer the requirements for the IT budget submissions prior to the annual Planning, Programming, Budgeting and Execution memorandum in accordance with the flow chart in MD 1400.

b. Reviewing and approving the Components' IT budget submitted into the DHS budget.

D. The ***Component Chief Information Officer*** is responsible for:

1. Timely delivery of mission IT services in direct support of Component mission, goals, objectives and programs.

2. Effective management and administration of all Component IT resources and assets to meet mission, Departmental and enterprise program goals. This will include:

IT Acquisitions (in excess of $2.5 Million):

a. Ensuring that prior to forwarding the procurement request (may be in a SLA, PR, IAA, etc.) to the contracting office for the acquisition of any IT equipment, software, services, or programs in excess of $2.5 million; the DHS Chief Information Officer has approved the acquisition.

b. Ensuring that these acquisitions are aligned with the Administration and Congressional priorities, and the DHS Chief Information Officer in advance to prevent an untimely delay in the purchase or acquisition.

c. At his/her discretion, instituting a lower threshold for DHS Chief Information Officer approval.

d. Requiring Acquisition Risk Audits be performed in accordance with Government Accountability Office (GAO) Report GAO/IMTEC-8.1.4 Information Technology: An Audit Guide for Assessing Acquisition Risks

e. For those purchases under $2.5 million, the Component CIO will approve these with in their respective Components, and provide a monthly report of these approvals to the CIO within ten (10) working days from the end of each month.

3. Compliance with all Departmental IT policies, processes, standards, guidelines and procedures.

4. Developing and reviewing the Component IT budget formulation and execution. This will include:

IT Budget:

a. Preparing a separate IT budget for information technology, starting with Fiscal Year 2009, using the annual Planning, Programming, Budgeting and Execution memorandum provided by the DHS Chief Financial Officer. This will include the IT budget across all programs and activities within the Component.

b. Working through the Component Financial Officer, submitting the IT Budget to the DHS Chief Financial Officer as part of the normal Planning, Programming, Budgeting and Execution process.

5. Accurately translating the business requirements of the Component into IT requirements.

6. Communicating with and educating the Component head and Component leadership team regarding the DHS Chief Information Officer Council priorities and initiatives.

7. Communicating with and educating the DHS Chief Information Officer and Chief Information Officer Council on the priorities and initiatives of the Component, and functionally supporting the DHS Chief Information Officer.

8. Developing and implementing the detailed enterprise architecture and detailed IT strategic plan, in consort with the DHS Chief Information Officer, specific to the Component's mission and in support of the DHS mission, as an integral component of the DHS enterprise architecture and the DHS IT strategic plan.

9. Implementing mission applications consistent with the DHS enterprise architecture.

10. Developing and maintaining a Component information security program that is fully aligned with the Department.

11. Ensuring mission IT solutions are secured and comply with the Departmental information security program.

12. Fully participating and engaging with the Chief Information Officer Council and Enterprise Architecture Board and supporting the Chief Information Officer Council decisions.

13. Collaborating with the DHS Chief Information Officer or senior enterprise IT official to ensure IT programs and policies optimize mission effectiveness and success.

14. Acquiring, developing, operating and maintaining all mission related systems and services.

15. With their Component head and the DHS Chief Information Officer, ensuring appropriate IT resources are made available for enterprise IT services and solutions.

E. ***Each senior enterprise IT official*** is responsible for:

1. Directing activities in accordance with laws, regulations, this MD and as assigned by the Program Director and DHS Chief Information Officer.

2. Timely delivery of enterprise IT services and solutions in support of the enterprise program.

IT Acquisitions (in excess of $2.5 Million):

a. Ensuring that prior to any acquisition (may be in a SLA, PR, IAA, etc.) of IT equipment, software, services, or programs in excess of $2.5 million; the DHS Chief Information Officer has approved the acquisition.

b. Ensuring that these acquisitions are aligned with the Administration and Congressional priorities, and the DHS Chief Information Officer in advance to prevent an untimely delay in the purchase or acquisition.

3. Developing the IT budget, resource plan, IT program plan and IT performance metrics for the supported enterprise program.

IT Budget:

a. Preparing a separate budget for information technology, starting with Fiscal Year 2009, using the annual Planning, Programming, Budgeting and Execution memorandum provided by the DHS Chief Financial Officer.

b. Working through the Component Financial Officer, submitting the IT Budget to the DHS Chief Financial Officer as part of the normal Planning, Programming, Budgeting and Execution process.

4. Submitting for approval all enterprise solutions with affected Component Chief Information Officers to ensure Component mission needs are met and that enterprise activities are integrated and resourced appropriately and where appropriate, to deliver DHS mission objectives.

5. Collaborating with fellow Component Chief Information Officers and Component heads to ensure program success.

6. Acquiring, developing, operating and maintaining all enterprise related systems and services in accordance with this MD.

7. Complying with Departmental direction, guidelines, standards and policies that guide IT development and deployment.

8. Ensuring enterprise IT solutions are secured and comply with the Departmental information security program.

9. Developing the detailed enterprise architecture and IT strategic plan specific to their mission and in support of the DHS mission, as an integral component of the DHS enterprise architecture and the DHS IT strategic plan.

10. Implementing enterprise IT services and solutions consistent with the DHS enterprise architecture.

F. The ***Chief Information Officer Council*** is responsible for:

1. Ensuring development of information technology resource management policies, processes, best practices, performance measures and decision criteria for managing the delivery of information technology services and investments, while controlling costs and mitigating risks.

2. Establishing, resourcing and funding centers of excellence, boards and working groups tied to the Chief Information Officer Council priorities.

3. Developing and executing formal communications programs for internal and external constituencies.

4. Providing recommendations for:

a. Establishing a Departmental IT strategic plan.

b. Setting priorities for the information technology function.

c. Resource sharing.

d. Coordination and consolidation of Component projects and activities.

e. Implementation of shared IT services.

f. Information sharing with other Federal, State, local, tribal and private sector entities.

g. Funding of enterprise information technology solutions.

h. Defining and continuously improving DHS information technology governance structures, processes and performance.

i. Coordinating and implementing an acquisition strategy for the delivery and maintenance of information technology solutions.

j. Establishing milestones, timelines and SLAs for IT integration plans.

5. Designating IT services and solutions as enterprise IT services and solutions.

G. The ***Enterprise Architecture Board (EAB)***, in support of the DHS investment review process, is responsible for the following:

1. Reviewing, making recommendations to the DHS CIO for approving individual investments consistent with the criteria and thresholds identified in DHS Management Directive 1400, Investment Review Process.

2. Requiring that each IT investment aligns with the DHS enterprise architecture and is approved by the EAB before submission to the CIO for final approval and inclusion in the annual budget submission.

3. Directing, overseeing and approving the DHS enterprise architecture and ensuring compliance with the Office of Management and Budget (OMB) Federal Enterprise Architecture (FEA) guidance.

H. The ***DHS Chief Information Officer*** and the ***DHS Chief Procurement Officer*** will jointly establish a system to ensure that any purchase request or document authorizing the acquisition of any IT equipment, services or programs in excess of $2.5 million is approved by the DHS Chief Information Officer, through the Component Chief Information Officer.

I. The ***Chief Financial Officer*** will specify the format of the budget submission in the annual Planning, Programming, Budgeting and Execution memorandum, starting in the Fiscal Year 2009 - Fiscal Year 2013 cycle, and will forward the Components' IT budget submission to the DHS Chief Information Officer for review and approval per the timeline identified in the Planning, Programming, Budgeting and Execution memorandum.

VI. Policy & Procedures

A. ***Policy***:

1. It is the policy of DHS that the CIO shall serve as the foundational DHS organization through which all Department-wide IT activities and services will be overseen, defined and measured. DHS will standardize IT policies across DHS to ensure functional excellence.

2. Authority and accountability for integration: The DHS Chief Information Officer, collaborating with the Chief Information Officer Council and its centers of excellence, designs, directs and oversees the implementation of the integration of IT across the Department to improve mission support quality and efficiency. Component heads, Component Chief Information Officers and the DHS Chief Information Officer all share accountability to the Under Secretary for Management for successful planning and implementation of functional integration and adherence to this MD.

B. ***Principles***:

Functional integration will rely on the following principles:

1. Focusing on the Mission.

2. Recognizing our employees as our most valuable asset and making the investments in their career development and professional growth.

3. Planning rigorously and implementing when success is likely.

4. Continuously assessing and improving operational effectiveness.

C. ***Procedures***:

1. Standardization and consolidation: DHS will standardize appropriate IT procedures across the Department to ensure functional excellence (this will be an ongoing effort).

a. Systems: DHS will continue to consolidate and integrate the number of systems supporting the Department's IT functions, ensuring such action results in efficiencies and does not compromise mission effectiveness.

b. Organizations: A guiding principle of the DHS Chief Information Officer will be to consolidate the number of organizations that perform the same function and create centers of excellence, ensuring such action results in efficiencies and does not compromise mission effectiveness.

2. Integration milestones: The DHS Chief Information Officer, in collaboration with the Component heads and Chief Information Officer Council, will annually establish milestones for the functional integration of IT.

3. Performance metrics: The DHS Chief Information Officer ensures the use of Department-wide performance standards and metrics and appropriate reporting systems. These metrics and reporting systems establish and measure performance, IT functional objectives and external benchmarks for all DHS Components. To track progress and to monitor Component Chief Information Officer and IT organizations, the DHS Chief Information Officer will annually assign certain key performance metrics to Component heads and Component Chief Information Officers. Some suggested performance metrics will be relevant to all DHS Components and some will differ by Component.

4. Enterprise IT services and solutions: The Department will continue to consolidate and integrate the number of IT systems supporting the Department's enterprise business processes as defined by the DHS enterprise architecture (e.g., Human Capital, Financial Management, Acquisition and Procurement, Administrative Services, IT Infrastructure). Enterprise IT services and solutions may be delivered to DHS Components via:

a. Centralized service provider: One office deemed to be a "Center of Excellence" and designated as the provider of the service for all DHS Components.

b. Shared service provider: Several Components, deemed to be "Centers of Excellence," are designated to provide IT Services to themselves and other Components.

c. External service provider: An external entity that provides IT services.

d. Other or hybrids: Possible combinations of the above or service provided by some other mechanism to be determined.

e. These services may be provided by government employees, contractors, or a mix, whichever is most efficient and effective.

f. Future MDs or policy directives will be developed by the Chief Information Officer to define performance standards and metrics for enterprise IT services and solutions.

5. Mission IT services: DHS will continue to consolidate and integrate the number of IT systems supporting the Department's mission processes as identified by the DHS Enterprise Architecture and approved by the Component heads or the DHS investment review process, or as otherwise directed by law and Executive Order.

6. Service Level Agreements: The DHS Chief Information Officer is responsible for overseeing the development of SLAs that define appropriate levels of service and compensation between Components that require enterprise IT services and solutions and the IT service providers. The DHS Chief Information Officer ensures that accountability and pricing is clearly defined, that customer problems are resolved promptly and that SLAs are meaningful, supportable and executable. The DHS Chief Information Officer ensures performance is measured and appraised for all IT service providers. All SLAs between DHS Components and support service providers (both internal and external) will include:

a. Resources required

b. Performance period

c. Performance metrics and reporting

d. Responsibilities

e. Funding mechanism

f. Terms and pricing for services

g. Dispute resolution process

h. Corrective action plans

i. Termination policy

j. Continuous improvement goals

k. Signatures of the responsible official for the provider, the receiver of service, and the DHS Chief Information Officer

l. Other content as determined by the Chief Information Officer Council

D. ***Implementation*** of these policies and programs may be delegated, when necessary, to managers and supervisors responsible for managing assigned personnel. Managers and supervisors at all levels are accountable for the execution of responsibilities within the framework of Federal and DHS policies.

VII. IT Infrastructure

IT Infrastructure is defined as all of the elements employed in the delivery of IT services to users, including the computing, network and telecommunications hardware, software, database management and operating systems software, middleware, help desk, Network Operations Center (NOC)/Security Operations Center (SOC), people, documentation and video. The infrastructure is a shared resource, the state of which bounds the adaptability and change capacity of the Department.

A. The DHS CIO shall serve as the foundational DHS IT organization and shall provide guidance, direction and over sight of the delivery of all IT infrastructure services for the Department, including policy and standards for definition, management, delivery and measurement of IT services.

B. The DHS Chief Information Officer shall define IT infrastructure goals and objectives and shall direct all IT Infrastructure efforts necessary to achieve those goals and objectives.

C. The DHS Chief Information Officer, working through the Infrastructure Transformation Program Office, shall direct the consolidation and optimization of DHS IT infrastructure equipment, services, people and processes to improve IT interoperability value delivery in support of the DHS mission and where feasible, achieve cost savings.

D. Consistent with the DHS investment review process, recommendations for IT Infrastructure investments and operations and maintenance funds throughout the Department shall be provided to DHS leadership by the DHS Chief Information Officer, with input from the Component Chief Information Officers. IT Infrastructure investments will be managed through a centralized DHS process.

E. The DHS Chief Information Officer shall report semi-annually to the Office of the Secretary and all Component heads on the state of the DHS IT Infrastructure.

F. The DHS Chief Information Officer, with the support of the Chief Information Officer Council, will ensure that IT Infrastructure services are provided in support of all Departmental and Component missions through service delivery models as outlined in Section VI.C.4.

G. In order to provide clear boundaries and quantifiable performance metrics, the DHS Chief Information Officer (with assistance from the Chief Procurement Officer) will implement SLAs for all DHS IT Infrastructure services and deliverables. These SLAs will be executed annually between the DHS Chief Information Officer and each Component head and Component Chief Information Officer.

VIII. Questions

Questions or concerns regarding this MD should be addressed to the DHS Chief Information Officer.

Michael Chertoff
Secretary of Homeland Security

2/15/07
Date

ADDENDUM A

INFORMATION TECHNOLOGY PORTFOLIO MANAGEMENT

I. Purpose

This addendum establishes DHS policies and assigns the responsibilities for the management of IT investments using portfolio management processes, methodologies, and techniques.

II. Policy

A. The DHS Chief Information Officer shall direct and oversee the implementation of IT Portfolio Management processes.

B. Defining portfolio criteria and creating IT portfolios

1. IT Portfolio Management processes shall define DHS IT portfolios by developing groups of related DHS IT investments and assets into portfolios based on DHS mission areas, strategic goals, objectives, and infrastructure requirements, irrespective of organizational boundaries. Processes to manage these portfolios should ultimately improve visibility into the relationships and interfaces between investments, reduce duplicative investments in systems and platforms, and enable the Department to more effectively allocate resources to provide the greatest benefit to the enterprise.

2. IT Portfolio Management processes shall establish performance goals for each portfolio, measure the performance of each portfolio, and continuously improve the balance of IT investments within each portfolio to more effectively meet established performance goals.

3. IT Portfolio Management processes shall use the DHS enterprise architecture to assess alignment of portfolios to DHS mission areas, strategic goals, objectives, and infrastructure requirements. In addition, these processes should use the DHS enterprise architecture to establish overall performance goals for each portfolio.

C. Evaluating IT portfolios

1. IT Portfolio Management processes shall leverage and support existing DHS IT investment decision forums and governance structures (e.g., Investment Review Process; Planning, Programming, Budgeting, and Execution process, etc.).

2. Existing investment decision forums should draw upon portfolio-level analysis during critical investment and acquisitions reviews. In addition, IT Portfolio Management processes should leverage, to the extent possible, investment-level analysis obtained from existing investment decision forums.

III. Responsibilities

A. The ***DHS Chief Information Officer*** is responsible for:

1. Establishing repeatable IT portfolio management processes, including supporting governance structure(s), consistent with the policies contained herein. The processes shall be communicated widely and cascaded down to the DHS Components so that they can understand expectations and effectively participate in the process.

2. Defining IT portfolios and adjusting them based on evolving DHS mission areas, strategic gods, priorities, objectives, and infrastructure requirements.

3. Designating portfolio managers for each IT portfolio.

4. Providing portfolio managers and other key stakeholder access to appropriate budget, program, EA, acquisition and investment documentation to support portfolio management efforts.

5. Partnering with Component CIOs' to establish the DHS IT portfolio management processes at their respective Component.

6. Establishing an effective program and project management discipline and providing quarterly performance reports to leadership.

7. Establishing appropriate change management strategy to effectively implement portfolio management across the department.

B. ***Portfolio Managers*** are responsible for:

1. Applying DHS IT Portfolio Management processes established by CIO.

2. Providing oversight of investments within portfolio, including:

a. Providing recommendations to CIO and other established investment governance boards for IT investments with their portfolio

b. Working with EAB and Chief Information Security Officer (CISO) to ensure alignment of portfolio to CIO and departmental goals

3. Supporting IT budget formulation, including:

a. Consolidating and reviewing IT budget submission for investments within the portfolio as part of the normal Planning, Programming, Budgeting, and Execution process

b. Coordinating evaluation of proposed investments in the portfolio

c. Coordinating evaluation of portfolio investments with Component IT program managers

4. Reviewing IT acquisitions and performance, including:

a. Participating in CIO review of IT acquisitions over $2.5 million

b. Reviewing periodic cost, schedule, and performance reporting for investments within portfolio

c. Leading portfolio performance reviews

5. Supporting the development and implementation of Enterprise Architecture targets and transition plans for their respective portfolio, including:

a. Coordinating with the CIO and EAB to establish architectural targets for the portfolio, including target capabilities, services, and technologies

b. Proactively evaluating balance of investments and systems within portfolio to ensure appropriate progress against established targets

C. The ***DHS CIO Council*** is responsible for:

Facilitating coordination among designated IT portfolio managers and IT programs.

D. ***Component heads*** are responsible for:

Ensuring the Component participates in the execution of the IT portfolio management process.

E. The ***Component Chief Information Officer*** is responsible for:

1. Facilitating coordination among designated portfolio managers and their Component IT programs as required by IT portfolio management processes.

2. Ensuring that DHS IT portfolio management processes are implemented at their respective Component.

ADDENDUM B

SENIOR INFORMATION TECHNOLOGY INFRASTRUCTURE OFFICERS COUNCIL

I. Purpose

The consolidation and migration of the DHS Information Technology (IT) infrastructure is paramount to not only the successful unification of the Department of Homeland Security (DHS), but to enable DHS to provide effective information sharing and IT security. This addendum defines the scope of authority for the Senior Infrastructure Officer (SIO) Council, and identifies its responsibilities and operating procedures. In addition, the SIO Council is charged with supporting and executing the planning and sustainment of the Department's integrated enterprise IT services (DHS One-Infrastructure), as directed by the DHS Chief Information Officer.

II. Responsibilities

A. The ***DHS Chief Information Officer***:

1. Directs the DHS Director of Information Technology Services Office (ITSO) to implement a Senior Infrastructure Officer Council to support the consolidation and coordination of the IT infrastructure.

2. Provides performance-rating input/feedback for Component SIO Council members to the Component Chief Information Officer (CIO) as well as recommendations and/or other forms of commendation.

B. The ***Component Chief Information Officers*** are responsible for appointing the component Senior Infrastructure Officer.

C. The ***DHS Director, ITSO*** chairs the SIO Council and is responsible for:

1. Providing overall leadership and direction in collaboration with the SIOC – for the design, development and implementation of optimum structure, processes and systems.

2. Providing the Office of the Secretary and Component Heads an annual evaluation of Infrastructure Transformation Program performance to include an assessment of each Component's functional performance.

3. Overseeing the development of reimbursable agreements for cross-Component ITP efforts where required. Once an agreement is coordinated, presenting it to the appropriate parties for their signature.

4. Presiding over SIO Council meetings.

5. Approving the agenda for SIO Council Meetings.

6. Providing SIO Council leadership and direction.

7. Assigning action items.

8. Overseeing activities of subordinate bodies formed by the SIO Council.

9. Reporting to the Chief Information Officer (CIO) Council on SIO Council activities.

10. Presenting SIO Council recommendations and open remaining issues to the CIO Council for approval and resolution.

D. The ***SIO Council*** is composed of the SIOs, who are the representatives of the Component Chief Information Officers. These SIOs are experienced IT professionals who have a broad IT experience. The SIO Council representatives are responsible for keeping their Component's Chief Information Officer apprised of issues affecting their respective Component IT infrastructure migration efforts. To represent these issues to the SIO Council, component representatives are responsible for obtaining the concurrence of their Components' Chief Information Officer with regard to matters under consideration by the SIO Council. In addition, the SIO Council representatives have the following responsibilities:

1. Representing technology interest in support of the Component's business operations.

2. Providing Component requirements and priorities for enterprise-wide IT services to the SIO Council.

3. Providing status of actions and milestones for infrastructure transformation and follow-on life-cycle operation & maintenance, and technology refreshment to the SIO Council.

4. Providing Subject Matter Experts (SMEs) to participate in the life-cycle development reviews, including the review of technical and operational designs, project costs, and schedules.

5. Formulating recommendations and analyze issues for presentation to the CIO Council.

6. Serving as the principal point of contact (POC) for their Component regarding IT infrastructure transition and integration efforts.

7. Serving as liaison between their Component Chief Information

Officer, Steward Organizations (Steward Organizations are the Components that provide certain enterprise-wide services to DHS; for instance, CBP provides Network services to the Department) and the Infrastructure Transformation Program Management Office, ensuring that action items are properly coordinated and/or assigned and carried out by their Component organization.

8. Ensuring their respective Component is actively engaged and represented on the Steward Working Groups and that information/decisions emerging from the Steward Working Groups is brought to the SIO Council for information and action, if necessary.

9. Providing feedback to their CIO and other Component stakeholders on SIO Council activities and direction.

10. Promoting the CIO Council and SIO Council strategy and decisions both within their organization and externally.

E. The ***Director, Infrastructure Transformation Program Management Office*** has the following responsibilities:

1. Maintaining a current roster with contact information of all officially designated SIO Council representatives (primary and alternate) including the record copies of designation forms signed by the Component CIO or equivalent/senior level official.

2. Supporting SIO Council meetings (e.g. develop draft agenda for approval by the Chair, prepare meeting materials, prepare and distribute meeting minutes).

3. Ensuring that all Components have the opportunity to address their concerns during sessions.

4. Facilitating the SIO Council meetings at the discretion of the SIO Council Chair.

5. Managing all SIO Council action items.

F. The CIO Council may establish sub-working groups. The chair of each sub-working group will be designated by the SIO Council Chair. Sub-working groups will:

1. Be either standing or temporary as deemed necessary.

2. Address IT infrastructure transition and migration issues within a specific service area (e.g. Network Service, Data Center Services).

3. Report progress and provide recommendations to the SIO Council.

III. Policies and Procedures

A. Policy:

1. The SIO Council is comprised of the ITSO Director, ITP Director, one primary and one alternate representative from each Component designated in writing by the Component CIO or equivalent staff principal. The primary representative from each Component is the SIO for the Component. These primary and alternate representatives are government employees. The Infrastructure Transformation Program Management Office shall provide appropriate personnel to serve as support staff for the SIO Council.

2. SIO Council representatives are authorized by their Component CIO to act as their decision-making representative for any ITP issue that may come before the SIO Council.

3. The SIO Council takes direction from, and in turn provides advice and recommendations to, the CIO Council in order to drive the IT infrastructure integration agenda of the Department.

4. The SIO Chair or his/her designated representative presents SIO Council recommendations to the CIO Council. Any representative whose Component does not concur with the consensus of the SIO Council as presented by the SIO Council Chair will have recourse to either request that the SIO Council Chair include the basis for their non-concurrence in the presentation to the CIO Council or to have their respective Component CIO do so.

5. The SIO Council representatives vote on major issues as determined by the Chair. Each organization present (in person, on the phone, or via video teleconference) at the meeting has a single vote including the Chair and the ITP Director.

B. Procedures:

1. Component SIOs work collectively to manage the meeting agenda and address the items based upon priorities established by the Chair, the CIO Council and the SIO Council. If there is a disagreement between the Chair, the CIO Council and the SIO Council, the CIO Council prevails.

2. SIO Council read-ahead materials are distributed a minimum of two business days prior to the meeting.

3. The Infrastructure Transformation Program Management Office records pertinent information, including members in attendance and decisions/actions associated during each SIO Council meeting. Action items assigned at meetings are recorded, tracked and managed by the Infrastructure Transformation Program Management Office under the guidance of the Chair to assure timely closure.

4. For Component transition reporting, the Component SIO:

a. Compiles the Component Transition Progress report, which includes updates regarding network, data center, e-mail and other transitions and is due in writing to the Infrastructure Transformation Program Management Office three business days prior to the SIO Council meeting.

b. Briefs their Component's transition progress during the SIO Council meeting in accordance with the standard format developed by the Infrastructure Transformation Program Management Office and approved by the SIO Council.

5. For Steward progress reporting, the Steward SIO:

a. Reports progress of Steward against their project milestones.

b. Identifies issues that must be addressed by Component SIOs to ensure progress towards the Department's goals and/or achieve required levels of service and cost targets during operations and maintenance.

6. SIO Council meeting minutes are distributed no later than five business days following the meeting.

7. Component and Steward Transition Progress Reports are stored, tracked and consolidated by the Infrastructure Transformation Program Management Office and used as a basis for periodic reports provided to the DHS CIO, the CIO Council, and the Under Secretary for Management for inclusion in the Investment Review Board.

8. Prior to and during regularly scheduled meetings, members may submit recommendations to the SIO Council for consideration. They may submit proposed meeting agenda items to the Infrastructure Transformation Program Management Office or the Chairman of the SIO Council.

9. If a designated member cannot attend a meeting, the alternate member may attend as the replacement (and voting member) for that meeting. If both are unavailable, a Component CIO designated tertiary may attend. ..

DHS INFORMATION TECHNOLOGY SECURITY PROGRAM

I. Purpose

The importance of establishing and implementing an aggressive and robust Information Technology (IT) Security Program cannot be over emphasized in these critical times. There are numerous directives that provide guidance to the Department of Homeland Security (DHS). National Institute of Standards and Technology (NIST) directives/guidelines and the Federal Information Security Management Act (FISMA) are to guide DHS. However, without a structure to ensure that a strong and effective organization is in place to implement security and mitigate risk, we are destined to fail. This addendum establishes DHS policies and assigns the responsibilities for the integration and management of the Information Technology Security Program's policies, methodologies, tools, and reviews.

II. Policy and Procedures

A. The DHS Chief Information Officer directs the DHS Chief Information Security Officer (CISO) to implement the DHS Information Security Program.

B. The CISO, under the authority of the DHS Chief Information Officer and public law, directs the implementation of the Department's Information Security Program.

1. The CISO defines, publishes and implements DHS information security policy and architectural guidance to ensure that mission owners have the data and resources required to enable secure information sharing.

a. Security Architecture Policy and Configuration Guidance define baseline configuration guidance in compliance with Federal Information Security Management Act (FISMA), NIST, and Office of Management and Budget (OMB) guidance. Configuration management and oversight processes should ultimately improve the Department's security posture and situational awareness.

b. The CISO establishes and manages a process for review and concurrence of all technology insertion programs/projects for alignment with the DHS Security Architecture and Homeland Security Enterprise Architecture (HLS EA).

2. Implements a departmental FISMA Compliance and Oversight program. As such, the CISO:

a. Establishes annual performance goals for each Component's information security program, measures the performance of each Component's information security program, and provides guidance on methods to continuously improve the security posture for each Component. Oversight processes ensure that DHS information systems are properly accredited and relevant deficiencies are corrected.

b. CISO reviews and validates information security artifacts.

c. Identifies, tracks, and monitors all deficiencies identified by information security and findings from the Office of Inspector General (OIG) and the Government Accountability Office (GAO); ensures that plans of actions and milestones are developed; and ensures that Components manage efforts until closure.

3. The CISO establishes and manages a process for in-depth review of all DHS operational systems every two years.

4. The CISO evaluates the Departmental and Component DHS information security posture. CISO leverages and supports existing DHS IT governance processes and structures including, but not limited to, Capital Planning and Investment Control (CPIC), Information Technology Acquisition Review (ITAR), and Budget Review in order to evaluate the information security program.

III. Responsibilities

A. The ***DHS Chief Information Officer*** is responsible for:

1. Overseeing the Information Security Program.

a. Appointing and overseeing the DHS Chief Information Security Officer (CISO).

b. Ensuring that DHS security programs integrate fully into the DHS enterprise architecture and capital planning and investment control processes.

c. Reviewing and evaluating the Information Security Program annually.

d. Providing input/feedback to the rating officials for Component CISO and Information System Security Managers (ISSMs) as well as recommendations regarding bonus or award recommendations, pay adjustments and other forms of commendation.

2. Establishing repeatable information security procedures including supporting governance structures, consistent with the policies contained herein.

3. Providing Component CISO, ISSMs and other key stakeholders (e.g., Component CIO and Information System Security Officers (ISSOs) access to appropriate information security documentation and tools to support information security efforts.

B. The ***Component Chief Information Officer*** is responsible for establishing, overseeing and implementing the Component's Information Security Program.

C. The ***DHS Chief Information Security Officer*** is responsible for:

1. Implementing and maintaining a Departmental FISMA compliant information security program.

2. Defining FISMA Compliance and Oversight requirements and performance metrics.

a. Providing recommendations to the DHS CIO regarding metric usage and priorities.

b. Providing reports to the DHS CIO and Component CIO regarding performance metrics and identifying areas for improvement.

3. Establishing qualifications for information security positions within the Department.

4. Monitoring component information security training programs and ensuring compliance with departmental requirements.

5. Supporting established IT Governance Processes and providing recommendations to the DHS CIO.

a. Participating in CIO review of IT acquisitions over $2.5 million and adjudicating conditions.

b. Conducting budget process, OMB 300, and Enterprise Architecture Center of Excellence (EACOE) reviews in support of the Investment Review and Planning, Programming, Budgeting and Execution (PPBE) Processes.

6. Providing input/feedback to Component CISOs and ISSMs regarding issues that affect Components.

7. Chairing the DHS CISO Council.

8. Exercising oversight responsibilities for enterprise security operations functions.

D. The ***DHS CISO Council*** is responsible for:

1. Coordinating and providing input on major DHS CISO information security policies and initiatives.

2. Providing recommendations for:

a. New enterprise information security policies and procedures.

b. Enterprise security tools.

E. ***Component CISO and ISSM*** are responsible for:

1. Directing Component information security programs in accordance with Management Directive 4300.

2. Ensuring compliance with departmental information security policies.

3. Ensuring that information security decisions are distributed to the ISSO and other appropriate persons within their Component.

4. Apprising the Component CIO of all pertinent matters involving the security of IT systems.

5. Appointing ISSOs as required.

ACCESSIBLE SYSTEMS AND TECHNOLOGIES' POLICIES

I. Purpose

Title 29 of the United States Code, Section 794d, "Electronic and Information Technology" (commonly referred to as "Section 508 of the Rehabilitation Act") requires that the Federal government make electronic and information technology (EIT) accessible to all people regardless of their disabilities. The important task of ensuring that federal employees and the general public can access EIT from the government will not succeed unless a strong review process is in effect. This Addendum establishes DHS policies and assigns responsibilities for the integration and management of the Accessible Systems and Technologies' policies, methodologies, tools, and reviews.

II. Policy and Procedures

A. The DHS Chief Information Officer directs the DHS Director of Accessible Systems and Technology to implementation of the Department's Accessible Systems and Technology Program.

B. The Director of Accessible Systems and Technology, under the authority of the DHS Chief Information Officer and public law:

1. Defines, publishes and implements DHS Accessible Systems and Technology policy and guidance.

2. Implements a Departmental Accessible Systems and Technology Oversight program.

3. Establishes annual performance goals for each Component's Accessible Systems and Technology program, measures the performance of each Component's Accessible Systems and Technology program, and provides guidance on methods to continuously improve it by:

a. Reviewing and validating artifacts.

b. Identifying, tracking, and monitoring all Section 508 deficiencies identified; ensuring that corrective plans of action and milestones are developed; and ensuring that Components manage efforts until closure.

4. Establishes and manages a process for in-depth review of all IT Section 508 programs.

C. The DHS Director of Accessible Systems and Technology evaluates the Departmental and Components' accessible systems and technology posture. The Director leverages and supports existing DHS IT governance processes and structures (e.g., Capital Planning and Investment Control (CPIC), Information Technology Acquisition Review (ITAR), and Budget Review) in order to evaluate the Accessible Systems and Technology program.

III. Responsibilities

A. The ***DHS Chief Information Officer***:

1. Directs the DHS Director of Accessible Systems and Technology to implementation of the Department's Accessible Systems and Technology Program

2. Ensures that DHS Accessible Systems and Technology programs integrate fully into the DHS enterprise architecture and capital planning and investment control processes.

B. The ***Component Chief Information Officers*** are responsible for ensuring that a Component Accessible Systems and Technology program is established and implemented within their Component.

C. The ***DHS Director of Accessible Systems and Technology*** is responsible for:

1. Defining Accessible Systems and Technology Compliance and Oversight requirements and performance metrics.

a. Providing recommendations to the DHS CIO regarding metric usage and priorities.

b. Providing reports to the DHS CIO and Component Chief Information Officers regarding performance metrics and identifying areas for improvement.

2. Establishing repeatable Accessible Systems and Technology procedures, including supporting governance structures, consistent with the policies contained herein.

3. Providing Component Section 508 Coordinators and other key stakeholders access to appropriate Accessible Systems and Technology documentation and tools.

4. Establishing qualifications for Component Section 508 Coordinator positions within the Department.

5. Providing performance-rating input/feedback for Component 508 Coordinators to the Component Chief Information Officer as well as recommendations and/or other forms of commendation.

6. Supporting established IT Governance Processes and providing recommendations to the DHS CIO.

a. Participating in CIO review of IT acquisitions over $2.5 million to ensure Section 508 accessibility requirements are included.

b. Conducting budget process, OMB 300 project management and performance results scorecard, and Enterprise Architecture Center of Excellence (EACOE) reviews in support of the Investment Review and Planning, Programming, Budgeting and Execution (PPBE) processes.

D. ***Component Section 508 Coordinators*** are responsible for:

1. Directing Component Accessible Systems and Technology programs within their Component.

2. Ensuring processes are in place for the development and testing of Component systems with Departmental Accessible Systems and Technology policies.

ENTERPRISE ARCHITECTURE MANAGEMENT

I. Purpose

To ensure that a strong IT infrastructure is formalized and maintained at the Department of Homeland Security (DHS), this Addendum provides policy on Enterprise Architecture (EA) and defines related roles and responsibilities for ensuring compliance with legislative and executive level guidance on EA.

II. Policy and Procedures

A. The DHS Chief Information Officer directs the DHS Chief Technology Officer (CTO) to implement the Department's Enterprise Architecture, Enterprise Data Management and Geospatial Program.

B. The DHS Chief Technology Officer implements the Department's Enterprise Architecture, Enterprise Data Management and Geospatial Program.

C. The CTO establishes annual performance goals for each Component's Enterprise Architecture, Data Management and Geospatial programs, measures the performance of each the Component's Enterprise Architecture program, and provides guidance on methods for continual improvement.

D. The Homeland Security Enterprise Architecture is an information asset that supports enterprise transformation by:

1. Enabling leadership to prioritize available resources to support mission functions;

2. Ensuring that mission requirements drive technology investments;

3. Identifying current DHS capabilities and performance gaps and projected future gaps;

4. Developing and sharing an enterprise-wide strategy across DHS; and

5. Leading the organization through the process of transforming the enterprise to achieve DHS Strategy.

E. The Homeland Security Enterprise Architecture is the authoritative enterprise-wide information resource that describes the mission and business functions of the DHS as well as the performance, data, applications, services, technology, information security and privacy considerations. It describes the current architecture, target architecture and transition strategy for attaining the target goals and objectives.

F. DHS is moving progressively towards an architected environment and is developing a single, integrated, and comprehensive EA.

G. The Homeland Security Enterprise Architecture complies with legislative mandates, federal initiatives and oversight requirements. Specifically, the Federal Enterprise Architecture (FEA) shall be used as guidance.

H. DHS Components that develop architectures at a more detailed level than the department EA shall demonstrate that they are consistent with the Homeland Security Enterprise Architecture. The DHS Chief Architect uses the Homeland Security Enterprise Architecture to monitor Components alignment to the FEA standards.

I. DHS Components provides periodic updates to the requisite Component-related information at the appropriate level of detail in the Homeland Security Enterprise Architecture and in accordance with guidance from the Enterprise Architecture Program Management Office (EAPMO).

J. All DHS information technology programs/projects, as well as those that have any IT elements, will align with a portion of the Homeland Security Strategies as described by the Homeland Security Enterprise Architecture EA.

K. DHS Components establish and manage a process for review and approval of all programs/projects for alignment with the Homeland Security Enterprise Architecture in accordance with the thresholds and decision authorities specified in the Management Directive 1400. “Investment Review Process.”

L. Through the Enterprise Data Management Office (EDMO), the Homeland Security Enterprise Architecture establishes clear and concise policy direction to ensure that enterprise data is visible, accessible and understandable to authorized users to support mission objectives.

M. Through the Geospatial Management Office and in accordance with Management Directive 4030, “Geospatial Management Office”, the Homeland Security Enterprise Architecture defines clear and concise guidance and standards for geospatial information and technology efforts.

III. Responsibilities

A. The ***<u>DHS Chief Information Officer</u>*** is responsible for:

1. Establishing the DHS Enterprise Architecture Program Management Office (EAPMO) and providing the necessary direction,

support and resources.

2. Appointing the Enterprise Architecture, Director who will also serve as the DHS Chief Architect.

3. Ensuring that the Enterprise Architecture, program complies with applicable laws, regulations, OMB and DHS policies and procedures, and has an effective governance process.

4. Issuing policy concerning the ongoing development and maintenance of the Homeland Security Enterprise Architecture.

5. Ensuring that all IT programs/projects are evaluated for compliance with the IT budget, capital planning and control (CPIC), and acquisition review processes, as well as closer alignment with IT Life Cycle Management/System Life Cycle efforts during pre-planning stages.

6. Providing performance-rating input/feedback for the Component lead Enterprise Architect, a lead Data Architect, and a lead Geospatial Information Officer to the Component Chief Information Officer as well as recommendations and/or other forms of commendation.

B. The ***Chief Technology Officer*** directs the following subordinates:

1. The DHS Director, Enterprise Architecture

2. The DHS Director, Geospatial Management Office

3. The DHS Director, Enterprise Data Management Office

C. The ***DHS Director, Enterprise Architecture*** is responsible for:

1. Establishing, planning and directing the DHS EA Program and ensuring proper governance and oversight.

2. Providing guidance for the development of architectures and incorporating them into the Homeland Security Enterprise Architecture.

3. Establishing and managing the central repository for the Homeland Security Enterprise Architecture and providing for enterprise-wide access to the repository.

4. Serving as the Department’s representative on all EA-related issues to inter-governmental and intra-Departmental bodies and forums.

5. Serving as the Chair for the Enterprise Architecture Center of

Excellence (EA COE), developing and updating the DHS Enterprise Architecture Board (EAB) Governance Process Guide, managing EA alignment reviews, providing EA COE with recommendations on alignment of programs/projects, and insertion of new technology standards to the Homeland Security Enterprise Architecture.

6. Maintaining a repository of DHS EA Board conditions levied on programs/projects, monitoring the status of resolution, and reporting outstanding conditions to the DHS Chief Information Officer and appropriate Component CIO for action.

7. Chairing the DHS Architects Working Group as a forum for coordinating, communicating and collaborating with Component Chief Architects.

8. Ensuring EAPMO review of all IT acquisitions in accordance with the IT Acquisition Review Process.

9. Planning and executing continuing improvements to the EA and the EA Program based on annual assessments using the OMB EA assessment framework.

D. The ***DHS Director, Geospatial Management Office***, is responsible for:

1. Providing oversight and assuring compliance with the DHS geospatial profile within the Homeland Security Enterprise Architecture in accordance with the authorities of DHS MD 4030.

2. Supporting the Homeland Security Enterprise Architecture through authoritative review and recommendations regarding all geospatial programs/projects as part of the EA alignment review process.

3. Ensuring that geospatial programs/projects incorporate approved geospatial policies, standards, and governance, regardless of investment level, to ensure interoperability and consistency in geospatial operations.

4. Coordination of the establishment and management of the Geospatial Information Infrastructure (an enterprise-wide geospatial data warehouse, which includes software, geospatial services and common geospatial foundation data).

5. Assisting, in partnership with the Enterprise Data Management Office, the establishment and adoption of geospatial data standards for information sharing and data management within DHS; coordinating standards and technology architectures with DHS Components and partners including Federal, State, local, and private-industry partners; and maintaining and advancing the Homeland Security Geospatial Data Model.

6. Chairing the DHS Geospatial Working Group to provide department-wide geospatial governance and oversight.

7. Acting as the Executive Secretariat for the Geospatial Positioning Navigation and Timing Executive Committee.

8. Establishing standards and polices for DHS grants related to geospatial technologies, quality assessments, and assurance of HLS community access to geospatial data developed through the grants process.

9. In coordination with the OCIO/Enterprise Business Management Office, establishing and implementing a geospatial portfolio management process for the DHS enterprise.

E. The ***DHS Director, Enterprise Data Management Office*** is responsible for:

1. Establishing and guiding the adoption of enterprise data management practices and standards for information sharing and data management within DHS.

2. Establishing, defining the roles and responsibilities, and chairing the Data Management Working Group (DMWG) in which each Component participates.

3. Developing and maintaining a Concept of Operation that guides DHS in data management practices and procedures based on this policy.

4. Facilitating the development of the technical standards for naming conventions, data structure, and syntax of data.

5. Facilitating the development of standards for data exchange across DHS including the development and registration of information exchange packages.

6. Recommending, developing and maintaining an enterprise Data Reference Model and architecture that enables the sharing categorization, integration and discovery of enterprise data as part of the Homeland Security Enterprise Architecture.

7. Developing and periodically collecting metrics, at a minimum on an annual basis, to review Component data management performance and practices.

F. The ***Component Chief Information Officers*** are responsible for:

1. Appointing the component Chief Architect and for providing resources for the execution of an EA Program.

2. Appointing a lead Enterprise Architect, a lead Data Architect, and a lead Geospatial Information Officer, or equivalent who act as the primary points of coordination with the DHS Chief Enterprise Architect, the Director of the DHS Enterprise Data Management Office and the Director of the DHS Geospatial Management Office respectively.

3. Communicating Departmental EA, Enterprise Data Management and Geospatial policies, processes and procedures throughout the Component and ensuring all Component employees and contractors are in compliance.

4. Certifying the sufficiency and completeness of Component information in the Homeland Security Enterprise Architecture annually prior to the submission of the Homeland Security Enterprise Architecture to the Office of Management and Budget.

5. Providing the resources to support the update of the Homeland Security Enterprise Architecture with Component EA information and the implementation of detailed architectures at the Component level while ensuring that they comply with the Homeland Security Enterprise Architecture.

6. Designating a Component Chief Architect or providing the resources for the execution of the functions of the Chief Architect.

7. Designating a Component Geospatial Information Officer or providing the resources for the execution of the functions of the Geospatial Information Officer, as necessary

8. Designating a Component Data Architect or providing the resources for the execution of the functions of the Data Architect.

9. Ensuring the review of all IT programs/projects for alignment with the Homeland Security Enterprise Architecture in accordance with the decision authorities and thresholds identified in DHS MD 1400 Investment Review Process. For those IT programs/projects over which the Component CIO has decision authority, the Component CIO shall certify that the IT programs/projects align with the Homeland Security Enterprise Architecture.

10. Providing monthly reports to the DHS CIO on the Component EA alignment reviews conducted, the outcomes of those reviews, and the status of any conditions levied on the programs/projects reviewed.

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

G. The ***Component Chief Architects*** are responsible for:

1. Maintaining the currency and quality of Component EA information in the Homeland Security Enterprise Architecture in accordance with guidance from the EA PMO.

2. Developing the Component EA in accordance with guidance from the EA PMO and ensuring the Component EA complies with the Homeland Security Enterprise Architecture.

3. Providing EA guidance to IT Program/Project Managers on the use of the EA for IT planning and requirements for EA alignment reviews.

4. Actively participating in the EA COE by reviewing all decision requests in accordance with EA COE review criteria and ensuring that there is no duplication with Component IT programs/projects in planning, development, or in the operations and maintenance lifecycle stage.

5. Ensuring implementation of EA alignment reviews by monitoring program/project artifacts for alignment with the Homeland Security Enterprise Architecture and report on conditions levied on non-conforming programs/projects.

6. Representing the Component in all Departmental and inter-governmental EA-related activities.

H. The ***Component Data Architects*** are responsible for:

1. Maintaining the currency and quality of Component EA data architecture and data management policies and standards.

2. Providing appropriate data, metadata and data management artifacts in a timely manner, according to availability and service level agreements.

3. Participating actively in the Data Management Working Group (DMWG) by reviewing all decision requests in accordance with DWMG review criteria and identifying potential duplication with Component IT programs/projects in planning, under development, or in the operations and maintenance lifecycle stage.

4. Representing the Component in all Departmental and inter-governmental Data Architecture-related activities.

I. The ***Component Geospatial Information Officers*** are responsible for:

1. Assuring Component compliance of the DHS geospatial profile within the Homeland Security Enterprise Architecture in accordance with the authorities of DHS MD 4030.

2. Ensuring that geospatial programs/projects incorporate approved geospatial policies, standards, and governance, regardless of investment level, to ensure interoperability and consistency in geospatial operations.

3. Actively participating and supporting the DHS Geospatial Working Group to provide department-wide geospatial governance and oversight.

4. Actively participating and supporting the Geospatial Positioning Navigation and Timing Executive Committee.

5. Representing the Component in all Departmental and inter-governmental geospatial related activities.