Homeland Security

March 16, 2007

MEMORANDUM FOR: Distribution

FROM: Secretary Michael Chertoff

SUBJECT: Management Directive 0007.1, *INFORMATION TECHNOLOGY INTEGRATION AND MANAGEMENT*

I have recently promulgated Management Directive 0007.1, *INFORMATION TECHNOLOGY INTEGRATION AND MANAGEMENT*. This management directive is much more than a basic update of the previous version – it represents the first major revision of a functional area to ensure the unification of the Department of Homeland Security (DHS).

This directive strengthens the roles and responsibilities of the DHS Chief Information Officer (CIO) and those of the Component Chief Information Officers. It enhances leadership accountability for the performance, budgeting, and expenditure of the Department's information technology (IT) resources. Information technology plays a critical role in the fulfillment of the Department's mission and accounts for approximately ten percent of our budget each year. Because we are so dependent on effective IT implementation and utilization, the Department's CIO must have the ability to guide and direct our most important IT investments.

Accordingly, some of the major changes in this directive are as follows:

1. Components must provide their IT budgets annually to the DHS Chief Information Officer for review; the CIO will then make recommendations to me for final budget submissions to the Office of Management and Budget.
2. Any proposed IT acquisition greater than $2.5 million must be reviewed and approved by the DHS Chief Information Officer. IT acquisitions are defined as services for IT, software, hardware, communications, and infrastructure.
3. Before IT investment proposals greater than $2.5 million are submitted to the DHS CIO for approval, the Department's Enterprise Architecture Board must approve the investment and certify its alignment with the Department's enterprise architecture.
4. The DHS CIO will approve the hiring of Component CIOs, as well as set and approve their performance plans, ratings, and annual award compensation.

In support of the authorities listed above and detailed in the attached directive, the DHS Chief Information Officer will review each component's IT budgets and expenditures and ensure their alignment in the following areas:

1. The Secretary's goals and priorities;
2. The Department's enterprise architecture;
3. Needs definition and business case alignment;
4. Privacy rules and regulations;
5. Section 508 (Accessible Systems and Technology) compliance;
6. Information security compliance; and,
7. IT infrastructure compliance.

Thanks to the hard work of thousands of the Department's IT professionals since DHS was stood up in 2003, we have made significant progress on IT security, network infrastructure, common software applications, and major initiatives such as US-VISIT. However, I am convinced we can do significantly more in these areas and am relying on all DHS employees to embrace the changes outlined in this directive and to work diligently to implement them.

The overarching goal of this directive and those that will follow is to maximize coordination and transparency of core business functions across all components, while preserving components' ability to fulfill their mission without an overly burdensome, centralized bureaucracy. This balance is not easily struck, and we will continue to fine-tune our business processes as necessary to achieve this balance. Over the next several months, I will be reviewing other core functional areas such as procurement, financial management, asset management, human capital, and information security to provide similar alignment.

Thank you for your service to our great Nation.

Distribution list:
Under Secretary for Preparedness
Under Secretary for Management
Under Secretary for Science and Technology
Under Secretary, Federal Emergency Management Agency
Commandant, U.S. Coast Guard
Commissioner, Customs and Border Protection
Assistant Secretary for Policy
Assistant Secretary, Office of Intelligence and Analysis
Assistant Secretary, Legislative and Intergovernmental Affairs
Assistant Secretary, Transportation Security Administration
Assistant Secretary, Immigration and Customs Enforcement
Director, Citizenship and Immigration Services
Director, United States Secret Service
Director of Operations Coordination
Director, Federal Law Enforcement Training Center
Director, Domestic Nuclear Detection Office
Director, Screening Coordination Office

U.S. Department of Homeland Security
Management Directives System
MD Number: 0007.1
Issue Date: March 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 III).

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 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 multi-year 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 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.

_____   2/15/07
Michael Chertoff   Date
Secretary of Homeland Security

MD # 0007.1