



**Homeland
Security**

Departmental Priorities for Information Technology

February 4, 2010

Office of the Chief Information Officer

DHS Information Technology (IT) priorities

1. Improve IT program performance
2. Accelerate data center consolidation and OneNet completion
3. Broaden and deepen Enterprise Architecture (EA)
4. Maintain cyber security focus, with particular emphasis on Identity Management (leverage of HSPD-12)
5. Foster improved internal and external information sharing
6. Ensure operational excellence
7. Bolster Federal Government IT employee base

Improve IT program performance

- Review all major IT programs (79) to evaluate program fundamentals and identify systemic issues causing significant risk that require immediate action (e.g., reconfiguring or even stopping programs)
- Establish proactive assistance for in-flight programs and work to institutionalize program management (PM) standards
- Mature IT governance structure



Significantly impact program success through improved execution, engineering approaches, and reduced risk

Accelerate data center consolidation and OneNet completion

Data Center consolidation

- Continue drive to reduce from 24 legacy data centers to two modern data centers

OneNet transition

- Complete Continental United States (CONUS) Wide Area Network (WAN) circuits transition to Networx
- Components to transition to Trusted Internet Connections (TICs) by the end of 2010



Achieve budget efficiency and enhance IT security

Broaden and deepen Enterprise Architecture (EA)

- Revamp DHS governance to reflect a functional (portfolio) approach
- Work to broaden and deepen mission and business segment architectures
- Strengthen EA capabilities by automating EA processes and implement tools to drive EA “self-service”

 Proper use of EA in DHS will significantly improve mission delivery and unification of the Department

Ensure operational excellence


- Develop Enterprise Requirements Management Program (including tools, training standards, and templates)
- Drive maturation of Enterprise Operations Center (EOC)
- Execute Enterprise License Agreements (ELAs)
- Define Enterprise service applications



Implementing operational best practices and monitoring tools is critical to ensure operational excellence

Maintain cyber security focus


- Update Enterprise Security architecture framework to ensure Defense-in-Depth through implementation of Trust Zones and rationalization of Active Directory
- Migrate all Components to Trusted Internet Connections (TICs)
- Further embed Federal Information Security Management Act of 2002 (FISMA) into programs as our standard way of doing business



Implementation of an enterprise IT security architecture will enable a significantly enhanced defense-in-depth ability to protect and respond to threats to DHS IT systems

Drive maturation of Identity Management (IdAM)

- Develop and implement Identity Management segment architecture in alignment with the Federal Identity, Credential, and Access Management (FICAM) standards/protocol
- Develop strategy and plan for Attribute-Based Access Control (ABAC)
- Develop IdAM service at the enterprise level that addresses “use cases” by portfolio and security requirements, including leverage of HSPD-12 for internal users



The complete solution will implement role-based access based on business rules and policy requirements, facilitated by multiple technology solutions

Foster improved internal and external information sharing

- Develop Sensitive But Unclassified (SBU) segment interoperability architecture
- Continue development of DHS Information Sharing Environment (ISE)
 - Begin development of business rules for information access and role-based identity management for the Law Enforcement and Intelligence communities
 - Strengthen enterprise Service Oriented Architecture (SOA) message framework
- Support expansion / institutionalization of the National Information Exchange Model (NIEM)



The key to success is engaging the mission communities in defining the business rules based on a premise of optimum dissemination of data

Bolster Federal Government employee base

- Execute IT OCIO Staffing Plan (approved 2009) to increase Federal employee base by more than 200
- Develop and implement an integrated DHS IT Strategic Human Capital Plan to improve staff retention and career planning across DHS IT community

 Ensure strong Fed leadership and oversight of IT across DHS