Table of Contents

1 Overview

Identity Management (IdM) has been identified as a strategic issue by the DHS Information Sharing and Collaboration Office (ISCO) and the Office of the CIO (OCIO). This requirements document has been developed to support project sizing (cost, schedule, and resource planning) by prospective implementing organizations.

1.1 Background and Overview

The United States Department of Homeland Security (DHS) consists of approximately 180,000 people and was established in 2002 to unify a number of national organizations and institutions involved with various aspects of securing our nation against terrorist attacks. This enormously complex task had to face an immediate challenge of making all these previously independent organizations and institutions work together and appear as one cohesive department with a common vision, complementary missions, and like objectives.

Since its inception, DHS has come a long way towards meeting this challenge. The Infrastructure Transformation Office (ITO) was formed to fulfill the vision of one network and one set of services for DHS over the long term, and a number of internal DHS programs were initiated including MaxHR, eMerge2, and US-VISIT to focus on certain aspects of achieving this same vision.

Another important factor of this vision is to establish a nationwide Information Sharing Environment to streamline investigations and to improve security and accessibility of information maintained within various DHS systems and application environments. Maintaining an accurate and up-to-date set of identity information is critical to all DHS components and programs to ensure only authorized individuals can access critical DHS applications and services, regardless of whether these individuals are federal employees, contractors, or authorized state or local officials.

1.2 Project Name

The name of the project is indicative of the service provided and establishes a high-level boundary for deliverables and activities considered in-scope for the effort.

The name for this project is:

- Identity Management (IdM)

Other names considered included:

- Enterprise Identity Management
- DHS-wide Identity Management
- Identity Management and Authentication
- Identity Management and Access Control

1.3 Mission Statement

The mission of Identity Management is to establish a DHS-wide Identity Management and Access Control (IdM) mechanism, i.e., the set of business processes and supporting infrastructure that enable the secure sharing of information as a component of a secure nation-wide Terrorism Information Sharing Environment. IdM associates access privileges with established credentials that may in-turn be used to ensure "need-to-know" access to applications. This is complementary to SmartCard (creation and management of personnel credentials) and ICE DIMC (creation and management of server credentials).

1.4 Objectives

The IdM will provide a centralized access control and information service to address key objectives in the following three categories:

1) Cost (Big) - We continue to pay per/user licensing fees after employees and contractors are gone
2) Security (Bigger) - We must circulate “Do you know these people” data calls in the absence of an authoritative people directory
3) Mission (Biggest) - We must ensure need-to-know access to a growing number of users with a proliferation of mobile devices being used for anytime-anywhere access to an increasing number of applications and resources

Project objectives include:

- Pool resources of DHS Components to fund enterprise-wide IdM solution
- Provide uniform, high-level of service in a cost effective manner
- Respond to Executive Orders and Presidential Directives calling for establishment of “information sharing foundation services”
- Free up resources for mission-critical initiatives that would otherwise be creating overlapping and duplicative capabilities

1.5 Key Terms and Definitions

DHS has defined Identity Management (IdM) as:

> *The set of business processes and supporting infrastructure that enables the secure sharing of information, i.e., a secure, interoperable nation-wide Information Sharing Environment*

For purposes of this report, IdM can be thought of as the combination of processes, technologies, and systems that:

- Accurately identifies and manages identity information on all users who need access to DHS applications services.
- Creates the required accounts for end-users and issues credentials to end-users
- Defines, controls, or manages access privileges for users

- Consistently enforces DHS security policies across multiple application environments to improve the security and privacy of identity information.

2 Functional Requirements

DHS Components and Programs have similar functional requirements for identity-related (IdM) services. Consolidation of these efforts into a uniform enterprise-wide IdM architecture holds the promise of freeing up resources for mission priorities and delivering a uniform, cost-effective service that eases future integration needs with the DHS infrastructure.

The following categories of IdM requirements were identified during the course of this requirements gathering effort:

1) Single Sign-On / Simplified Sign-On / Reduced Sign-On
2) Password Reset
3) Improved User Administration and Self-Service
4) Account Provisioning and Workflow Capabilities
5) Policy Management and Audit Requirements
6) Use of public key infrastructure (PKI) digital certificates to support confidentiality, digital signatures, and non-repudiation
7) Enterprise-wide Directory Services to support user profile repositories
8) Secure Collaboration Services

The table below identifies "common threads" emerging from requirements interviews and relates how these common threads lead to requirements that can be grouped into the general categories of IdM requirements listed above:

Interview Common Threads	**Corresponding Functional Requirement**							
	1	2	3	4	5	6	7	8
	SSO	PW	Adm	Prov	Audit	Cert	Dir	Col
1) Identities are primarily managed on an application-specific or platform basis	X	X	X					
2) Manual input is currently the predominant method for managing identities across DHS applications and platforms		X	X	X				
3) Identity information is not well-maintained across the various system and application environments and is inconsistent between systems						X	X	
4) Users are frustrated with the number of ids and passwords required for accessing various application environments	X	X						
5) Administrators are not notified on a			X	X	X		X	

timely basis as changes occur								
6) DHS policies are not well communicated or understood					X		X	
7) Policy enforcement is "spotty" at best					X		X	
8) Audit information is incomplete within some system environments					X			
9) Many Components and programs are duplicating efforts to address common IdM-related issues	X	X	X	X	X	X	X	X

Note: Requirements for PKI are outside the scope of this effort as they are addressed by an existing DHS intiative.

The following sections identify the common functional requirements for IdM services along with brief descriptions of the business benefits as well as references to other DHS documentation describing these requirements in more detail.

2.1.1 Single Sign-On/Reduced Sign-On

Presently within many DHS Components internal users are issued multiple user-ids (usernames, monikers) and passwords to control access to IT systems and applications. These users, with multiple usernames/passwords must authenticate and re-authenticate themselves to multiple systems several times a day. This creates a situation where gaining access to various application environments is burdensome and problematic (user forgets password). In many cases, users are issued additional credentials such as PKI certificates, secure tokens, and in the near future, all employees and contractors will be issued smart cards for accessing various DHS systems or facilities.

In order to improve end-user productivity, many components and programs have Single Sign-On (SSO) initiatives that are intended to minimize the number of user-ids/passwords individual users must manage and the number of authentication events individual users encounter during the course of performing their jobs.

SSO/Reduced Sign-On components include both web-based SSO for accessing multiple web applications and web server environments, and enterprise SSO for accessing web and non-web application environments including mainframe applications or other non-web fat client environments. Web-based SSO solutions typically rely on session cookies stored within web browser while enterprise SSO solutions are typically additional client software that must be installed on an end-users desktop. Both web-based access control and enterprise SSO were considered requirements within the eMerge2, MaxHR, ICE-US-VISIT, and other components and programs.

2.1.2 Password Reset

Nearly all Components and programs interviewed seemed to require individual end-user self-service password reset capabilities to reduce the number of calls to help desk personnel.

Web-based or phone-based voice recognition capabilities that allow validated users to reset their own passwords can have a dramatic impact on the staffing needs of operational support

organizations. Many password management vendors also provide "password synchronization" capabilities that automatically change passwords on other systems with identical password polices as the end-user resets their password through the central password reset service.

Only applications which are non-critical and required by all users (including network file/print services, the e-mail system, and the intranet web environments) should be included within the password synchronization environment. Other more critical or sensitive application environments should require the user to re-enter their password and provide a second authentication factor such as a smart card, secure token, or certificate before access to these systems is granted.

2.1.3 Tools to Improve User Administration

A majority of Components and programs identified critical needs for tools to better manage their user populations. These tools include self-service administration capabilities so end-users can manage some of their own attributes on their own, delegated administration tools that will allow individual Components or program application owners to control who has access to their system environments, and federation capabilities that will allow trusted external organizations such as other federal agencies or authorized State and local offices to manage their own users populations locally, eliminating the need for DHS to manage all these users within their own repositories.

Self-service administration, delegated administration, and federated identity capabilities should all be thought of as long-term requirements within DHS. While most components could rely on self-service administration for managing certain internal user attributes, components such as the Office for Domestic Preparedness could rely extensively on delegated administration tools that enable State or local representatives to manage identities within DHS repositories. Finally, organizations like DOJ and State and local law enforcement agencies will rely on federated identity capabilities to improve collaboration and information sharing between these separate organizations in a secure and effective manner.

2.1.4 Provisioning Tools

The enterprise-wide IT infrastructure should include provisioning and workflow capabilities to automatically provision and de-provision these additional accounts as employee or contractors enter or leave the agencies.

One proposed model for provisioning is based on the user initiating access requests by filling out web-based forms. This model is good for internal users who require approval from an application owner or manager before accessing various applications, but could also be useful in cases where additional information concerning the end-user is needed in order to make informed decisions concerning the end-user's privileges. A request-based provisioning model could also be extended to support external users who may request access to DHS applications in the future, whether these applications are under the eMerge2 umbrella or controlled by another OE or program.

2.1.5 Policy Management and Audit Requirements

DHS has very stringent security and auditing requirements. Mandates that must be adhered to include: Homeland Security Presidential Directive (HSPD) 12 and the enabling federal standard, Federal Information Processing Standard (FIPS) 201, the USA PATRIOT Act, as amended, of 2001, and other regional or country specific privacy regulations. Other sources of federal IT

governance have been endorsed by the DHS Chief Information Security Officer (CISO) for DHS enterprise-wide use, such as the National Security Systems Handbook, DHS Sensitive Systems Policy Pub 4300A, National Security System Policy Pub 4300B, and Management Directive 4300-1. The DHS Privacy Office has identified Privacy Requirements for IdM, including overall privacy guidelines. Information protection policies, password policies, authentication/access control/authorization policies, and privacy policies must all be considered firm requirements. These mandates and policies effect both technologies and business processes under which DHS must demonstrate compliance.

The foregoing indicates a requirement for DHS to implement a policy server within the infrastructure to embody policy enforcement. Policy enforcement engines allow for policies to be enabled and enforced across multiple application environments. Some policies must be defined and administered by a central authority such as the Office of the CISO, while other policies may apply to a specific Component, program, or application environment. Therefore, other security representatives or application owners from these organizations will also need access to the policy repository.

HSPD-12 and FIPS 201 include guidance from NIST and indicate that DHS must be able to support multiple levels of authentication assurance (Level 1 thru Level 4), defining the use of smart card authentication to IT systems. Smart cards are machine readable employee badges that contain a microprocessor chip on the card. All federal employees and contractors will be required to possess smart card identification cards that enable authentication at Level 4 as part of the federally implemented smart card program within the next few years. Caveat: external users will require multiple Level 1, Level 2, Level 3, and Level 4 authentication mechanisms for the foreseeable future.

DHS has a requirement to disable accounts and de-provision user accounts and facilities access within one (1) hour of an employee or contractor leaving the agency, or disable accounts and de-provision user accounts as changes occur (such as job changes) indicating they no longer need access to specific application environments. This indicates very strong auditing capabilities must be in place, including the capability to identify all accounts have been assigned to a particular individual, who authorized or approved actions for creating/disabling/or changing accounts and privileges, and actions/transactions initiated or performed by specific individuals, whether they are an internal DHS user or external party accessing DHS systems.

2.1.6 Enterprise Directory containing Quality Identity Data

Enterprise Directory services should be considered an important prerequisite to many of the functional requirements discussed above. The directory environment must store identity information (user profiles) concerning people, groups of people, organizations, roles, devices, and applications and support the LDAP and the directory services markup language (DSML) protocols.

The quality of the user profile identity data can be ensured by integrating a directory environment with other key repositories being deployed within DHS, including, but not limited to: Finance and Human Resource deployments, Active Directory, component or program specific LDAP repositories, and other web-based directories or application-specific /databases.

2.1.7 Secure Collaboration

Several DHS components and other Federal, State, and local agencies often need to exchange information in a secure manner to facilitate investigations or improve the level of service they provide. DHS must identify strategic DHS encryption packages, PKI technologies, web-based application integration standards, federation capabilities, and various eXtensible Mark-up Language (XML) based standards to enable secure document exchange and promote secure collaboration between components, programs, and with other trusted agencies/organizations. Detailed requirements for many of these capabilities are currently emerging or have already been identified in other DHS publications, other federal agency publications (such as U.S. General Services Administration, DOJ, U.S. Department of Defense, and others), and in standards body publications from organizations such as NIST and the Organization for the Advancement of Structured Information Standards (OASIS).

3 Information Needs

3.1 Classification and Privacy Considerations

Initial IdM capabilities shall

1) Support unclassified to Sensitive But Unclassified (SBU) environments. Subsequent releases must be able to support classified environments.
2) Enable DHS privacy strategy

3.2 Authoritative Sources of Information

To ensure its validity and consistency, information that will be provided to applications through the IdM services will be drawn from authoritative sources. It is expected that the IdM directory will need to make available data contributed by multiple authoritative sources. Furthermore, it is likely that the data needs of current and future applications will evolve over time. Therefore, it is important for DHS to have the ability to aggregate data from multiple sources (LDAP, databases, spreadsheets, etc.) and create customized "views" of data to meet any and all needs that may arise. This capability is often referred to as "Virtual Directories" or "virtualization" and should be considered an important requirement to ensure the directory infrastructure is flexible and extensible enough to meet current and future needs from the various DHS components and programs.

4 Technical Requirements

4.1 Enterprise Architecture Compliance

The IdM solution must be compliant with Homeland Security Enterprise Architecture.

4.2 Service-level Requirements

The IdM solution must be geographically redundant, fault-tolerant, and extremely accessible and reliable. Techniques such as functionality and availability monitoring will be important in ensuring that service levels are met. In addition, the IdM solution must provide consideration for simplifying future integration and deployment of web services, access management solutions, and provisioning solutions within the DHS infrastructure.

4.2.1 Technology Evaluation Criteria

The Department must prudently invest in technology that accommodates comprehensive identity management architecture, phased builds and releases, staged and incremental roll-out of functionality, standards-based interoperation with other systems, etc. To this end, the directory infrastructure, the centralized access request system, and necessary delegated administration tools have been identified as high-priority near-term needs.

The Department plans to rely, to the greatest extent possible, on commercial-off-the-shelf products in the marketplace that can support a set of salient features and operational parameters in the following areas:

- Directory Capability
- Access Management Capability
- Provisioning/Workflow/Auditing Capability

a) Directory Capability

Product(s) and release/version available as of 4/25/2005
Key Requirements
1) Performance and scalability, e.g., phased scaleability up to 2 million authentications/day
2) Standards Support (LDAP V3, LDIF, DSML, etc.)
3) Static and Dynamic Groups
4) Application integration (APIs, code samples, etc.)
5) Multi-master and filtered Replication
6) 3rd party product support

7) Active Directory (AD) login Integration
8) Integrate other Authentication methods
9) Support Virtual Directory Views
10) Schema Management
11) Administration Tools
12) User Management Tools
13) Flexible access control lists (ACLs) for controlling data access
14) "Sounds-Like" or fuzzy search capability
15) Browser-based Access
16) Synchronization or meta-directory capabilities with other key repository technologies used by DHS (Peoplesoft, AD, Smart Card DB, etc.)
17) User profile repository within LDAP directory
18) The ability to provide “white pages” capability of user profiles

b) Access Management Capability

Product(s) and release/version available as of 4/25/2005
Key Requirements
1) Delegated administration Tools
2) Self-service administration
3) Workflow Approvals
4) Support role and group administration, including dynamic and nested groups
5) Ease of administration
6) Support for mobile devices
7) Access management of Web and non-Web applications, i.e., ability to provide URL-based web-access control, ability to provide COM and DCOM (fat client) access control from a standard desktop microcomputer

8) Single Sign-On (SSO) Capability
9) Provide selected logout of SSO sessions
10) Support for DHS authentication mechanisms
11) Allow independent invocation of authentication and authorization functions
12) Support complex business rule processing
13) Support re-prompting of user for authentication
14) SmartRules capability and Enforce privileges at Policy Decision Point (PDP)
15) Access one of two LDAP instances based on loginID
16) Leverage existing role and group information from multiple sources, concurrently
17) Support attribute based dynamic and filtered access control in a flat directory
18) Federation Support (SAML, Liberty Alliance, WS-*), i.e., the ability to federate access control and authorization services
19) Support for DHS installed portals including but not limited to Plumtree, WebSphere, Cold Fusion, Aprimo
20) SDK for C, Java, Perl, VB, and XML interfaces
21) Auditing capabilities
22) Proxy and agent architecture
23) Ability to grant authorization permissions using role-based access control (RBAC)

c) Provisioning/Workflow/Auditing Capability

Product(s) and release/version available as of 4/25/2005
Key Requirements
1) Connector Requirements
2) NOS/Active Directory connector
3) Email connector
4) PS connector
5) Connector Development Tool (ADSI, Java, LDAP, XML, VS.NET, etc.)
6) Encrypted Communications with targets (SSL or other)
7) Support bi-directional flow from authoritative sources to subscriber systems
8) Support data normalization and transformations

9) Support for additional business logic and rules to resolve discrepancies
10) Password Management
11) Self-service reset
12) Challenge/response for forgotten passwords
13) Password Policy Enforcement
14) Password Sync. with target systems
15) Account Management
16) List Accounts assigned to individuals
17) Identify Orphaned Login Accounts
18) Track changes made on local systems
19) Automatically report/suspend questionable accounts with exclusions for service and batch accounts
20) Roll-back changes
21) Assign orphaned accounts to valid users
22) Dynamically calculate privileges based on roles/groups/attributes
23) Ability to query provisioning status by requestor
24) Assign users to one or more roles
25) Map roles to access privileges
26) Define and enforce privileges based on Policies/Rules
27) Derive OU and global groups
28) Derive AD home directory and access control privileges from additional attributes
29) Create unique shortname accounts for each user according to DHS Policy
30) Audit and Control
31) Logging and time stamps for all user and account mgmt. activities
32) Flexible reporting capabilities (list active accounts per system at any point in time, etc.)
33) Weekly reports of services provisioned and de-provisioned
34) Secure Log files (tamper-proof) in standard format
35) Ability to provide relevant auditing output based upon user behavior
36) Delegated Administration
37) Ability to delegate user admin, policy, groups, and acct. mgmt. workflow definitions to specified organizations

38) Secure/Filtered views and tailored reports based on identity
39) Workflow
40) Dynamic calculate workflow for managing accounts
41) Templates/Forms for on-boarding, changes, terminations
42) Ability to route registration requests to DHS sponsor
43) Multi-level approval support
44) Periodic approval reminders and escalation capabilities
45) Email notifications
46) Support for dynamic and scheduled (timed) tasks
47) Ability to defer approvals to others
48) Ability to integrate with other workflow solutions (invoke other processes in Notes, MQ Series, PS, other)
49) Ability to assign people to one or more teams
50) Support for strong credentials (PKI, SmartCards)
51) Support for LDAP directories
52) Distributed provisioning support for remote locations
53) Standards Support (SPML, XACML, WS-*)
54) Ability to provision/de-provision user accounts on multi-platforms and operating systems
55) Support for provisioning phones, office space, furniture, computing equipment

5 Organizational Participation

5.1 Organizational Coverage of Existing Requirements

The requirements in this document for an enterprise IdM service were derived from a high-level requirements study conducted by an IdM research team. The IdM research team collected information by using three data collection techniques: (1) interviews; (2) review of FY06 OMB Exhibit 300 submissions; and, (3) review of the EA-COE System and Technology Inventory database.

Interviews were conducted between late January 2005 and early March 2005 with key representatives from Components and programs. The initial high-level study interviewed twelve components to obtain an initial sampling of requirements as a means of accurately identifying common DHS requirements while minimizing team size and data collection time.

The following table identifies the components and programs that were interviewed, the number of OMB 300 submissions by component, and which components responded to the EA-COE survey:

Directorate	**Component**	Interview	OMB 300	Enterprise Architecture Inventory
Border and Transportation Security (BTS)				
	Customs and Border Protection (CBP)	**X**	**26**	**X**
	Immigration and Customs Enforcement (ICE)	**X**	**7**	**X**
	Transportation Security Administration (TSA)	**X**	**11**	
	Federal Law Enforcement Training Center (FLETC)			
	Animal and Plant Health Inspection Service (APHIS)			
	Office for Domestic Preparedness (ODP)	**X**		
	Consolidated Enforcement Environment (CEE)		**1**	
	US-VISIT	**X**	**1**	**X**
Emergency Preparedness and Response (EPR)			**10**	**X**
	Federal Emergency Management Agency (FEMA)			
	Nuclear Incident Response Team (NIRT)			
	Domestic Emergency Support			
	National Domestic Preparedness Office			
	Chemical, Biological, Radiological, and Nuclear (CBRN) Response Assets			
Information Analysis and Infrastructure Protection (IAIP)		**ISCO**	**10**	
	National Cyber Security Division (NCSD)			
	Homeland Security Operations Center (HSOC)			
Science and Technology (S&T)			**4**	**X**
	Chemical, Biological, Radiological, and Nuclear (CBRN) Countermeasures			
	Environmental Measurements Laboratory (EML)			
	National Biological Warfare (BW) Defense Analysis			
	Plum Island Animal Disease Center			

	SAFECOM			
Management			**13**	
	Acquisition			
	Legal			
	Personnel			
	Office of Chief Information Officer (OCIO)	**CISO Credentialing EA-COE IAD ITO**		
	Travel			
	Office of International Affairs (OIA)			
	Communication			
	Office of Chief Financial Officer (OCFO)	**eMerge2 MaxHR**		
	Bank Card Program			
	Records Management			
	Asset Management			
	Combined Federal Campaign (CFC)			
	Program Analysis & Evaluation (PA&E)			
United States Coast Guard (USCG)		**X**	**16**	
United States Secret Service (USSS)		**X**	**1**	
United States Citizenship and Immigration Services (USCIS)			**9**	**X**

- Interviews were also conducted with other agencies that interact with DHS components, including:
  - The U.S. Department of Justice (DOJ)
  - Representative sample of State and local agencies

Other potential interviews that were discussed but did not occur for various reasons include:

- Components
  - Federal Emergency Management Agency (FEMA)
- Programs
  - HSIN Collaborative Applications

5.2 Organizational Participation for Implementation

Technology alone will not meet DHS's needs. The IdM effort must consider:

1) Establishing an IdM governance board consisting of additional analysts, business representatives, and technologists from various DHS components and programs that will:
   a. Investigate component-specific or program-specific processes for managing identities,
   b. Develop a more cohesive enterprise-wide set of processes for on-boarding and terminating contractors,
   c. Identify DHS wide UID standards, and

   d. Determine authoritative sources and required data flows to/from other critical DHS repositories

2) Selecting a limited set of DHS components and programs for the initial deployment
3) Assigning business analysts to determine the detailed short-term and long-term requirements for participating components and programs
4) Acquiring vendor solutions and systems integration services to deploy the necessary technologies in a phased manner

5.3 Program/Project Interdependencies

The IdM project must interface with and leverage outputs from the following ongoing activities:

1) DHS Enterprise Portal
2) Smart Card / Credentialing
3) ICE Bridge-certified PKI
4) DOJ/DHS sponsored Federation (Shibboleth) proof of concept
5) Other IdM and directory services as identified

6 Exclusions, Assumptions, and Constraints

6.1 Exclusions

The following items are identified as out of scope relative to establishing an initial IdM capability. These items will be considered in overall IdM project planning but will not be included in an initial implementation to respond to near-term needs of DHS.

1) SSO for external users. External users with access to multiple DHS systems or applications may also require SSO capabilities, or at least "Reduced Sign-On" to minimize authentication events and improve their experience when interacting with DHS. However, specific external user requirements are considered out of scope as initial requirements.
2) DHS SSO with Other Departments. Various DHS components and programs have indicated a need for SSO with other agencies such as the DOJ and for State and local officials who collaborate with DHS on a regular basis; however, this is beyond the scope of the initial IdM capability.
3) Public Key Infrastructure. The following PKI-related capabilities are out of the scope of the initial IdM requirements:
    a. Use of PKI certificates within application servers for DHS web-based applications to support data encryption, integrity, host authentication, virtual private networking, signatures, and non-repudiation.
    b. Potential extension of the PKI Certificate Authority capability within ICE that cross-certifies certificates through the Federal PKI bridge hierarchy to meet all of DHS's needs and eliminate additional costs for obtaining certificates from outside trusted third parties (TTPs) such as VeriSign.
    c. Application or infrastructure use of techniques such as Certificate Revocation Lists (CRLs) or the On-line Certificate Status Protocol (OCSP) to validate certificates.
4) SmartCards and Credentialing. DHS has an in-progress effort to address HSPD-12 credentialing requirements
5) Federation (Shibboleth Pilot). The concept of a Federation has emerged from the Global Security Architecture Committee and has received growing interest from several federal, state, regional, and local systems. As a result a demonstration project has been proposed under the co-sponsorship of the Department of Justice (DOJ) and the Department of Homeland Security (DHS). The initial phase of this proof of concept will include participation from the Criminal Information Sharing Alliance Network (CISAnet), Pennsylvania Justice Network (JNET), and the Regional Information Sharing Systems Network (RISSnet). Others expressing interest in participating in the demonstration during follow-on phases include the California Department of Justice, Wisconsin Department of Justice, DHS's Homeland Security Information Network (HSIN) / Joint Regional Information Exchange System (JRIES), and the Automated Regional Justice Information System (ARJIS).

6.2 Assumptions

The following assumptions pertain to the performance of this project:

1) Using batch routines to synchronize directories. An alternative to Commercial-Off-The-Shelf (COTS) meta-directory or synchronization solutions would be to rely on nightly batch file feeds and internally developed scripts on various systems to reconcile data on a nightly basis. However, this approach will not be sufficient for DHS. COTS meta-directory and synchronization solutions update their connectors on a regular basis as products mature and new releases become available, placing the upgrade burden on the selected vendor and minimizing the impact on DHS resources. More importantly, the HSPD-12 mandate for disabling user accounts within one hour of termination implies that a more automated approach is required for propagating changes throughout the enterprise, although strict processes for updating some authoritative source on or before a termination event occurs will still be required.

6.3 Constraints

DHS stakeholders identified a number of design principles for the future Identity Management Infrastructure. The following list provides key principles that should be considered when selecting potential solutions:

a. The IdM design should be flexible and extensible to meet current and future anticipated needs

b. Reliability, availability, and performance of infrastructure components are crucial

c. Various hardware and software components introduced as part of an IdM capability must easily integrate with the existing infrastructure where possible

d. DHS will leverage existing authoritative sources where feasible when establishing the general-purpose directories

e. DHS components and programs will be required to leverage the enterprise-wide shared services for IdM or rely on accepted Federation standards for integrating with DHS IdM infrastructure services unless there is a compelling reason and demonstrated need to do otherwise

f. DHS' preference is to support open standards and avoid vendor proprietary solutions

g. The design should focus on meeting the most crucial DHS needs by the end of CY2005, and may defer other features until 2006 and beyond

h. DHS has a preference for well established vendors with large market shares, and would like to avoid solutions from multiple vendors if possible that place the burden of integration on DHS resources.

i. Cost and feasibility of deployment are always concerns within DHS

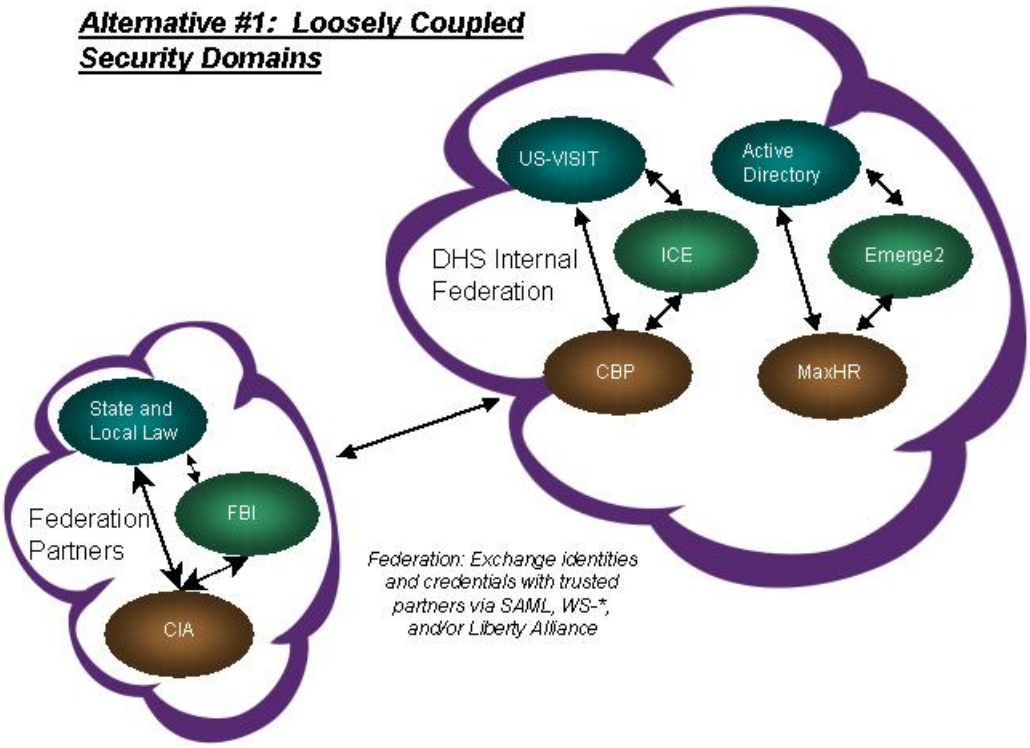
j. The new IdM infrastructure will be optimized as the framework for future application development and integration, while decisions to migrate legacy applications to leverage the new IdM framework will be made on a case-by-case basis during normal upgrade cycles

7 Alternatives Considered

DHS has already deployed some IdM technologies within the existing infrastructure, and has various mandates including HSPD-12 and OMB 300 that all components and programs must comply with. These initiatives and other component or program specific initiatives already underway provide DHS with many options for evolving the infrastructure over time to meet current and future needs.

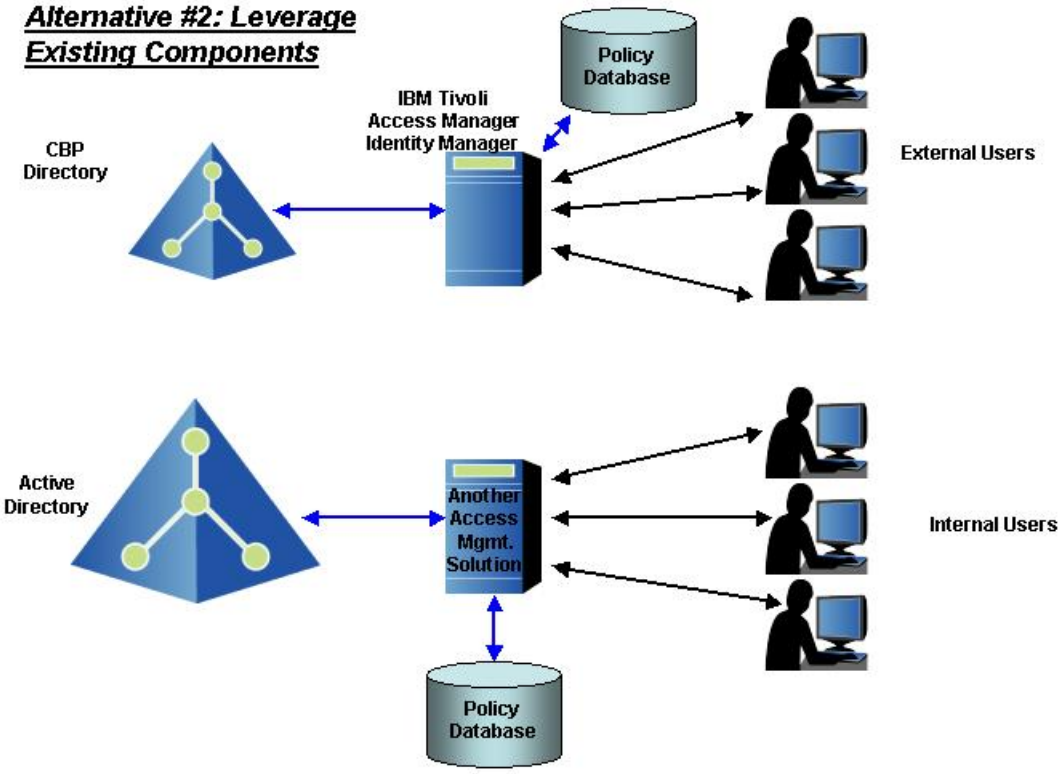
Three alternatives are described below. These are not the only options available and are provided as examples of possible courses of action. The recommended alternative must be justified by an alternatives analysis and cost-benefit analysis.

7.1 Alternative 1: Loosely Coupled Security Domains



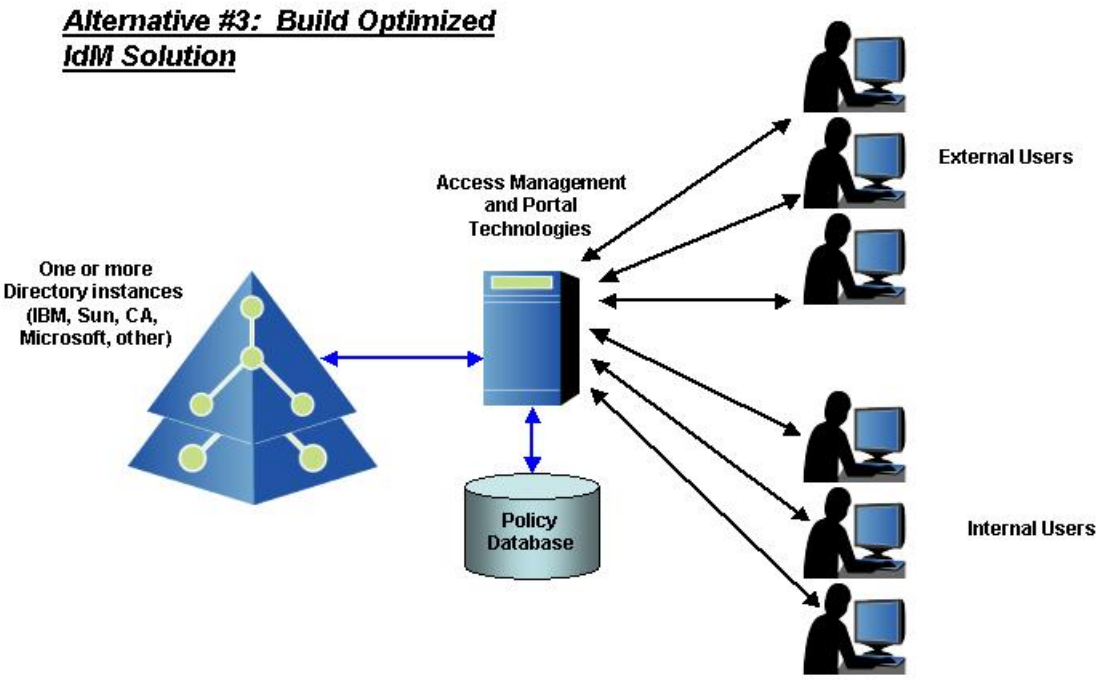
Advantages	Disadvantages
1) Causes the least disruption to existing DHS components and programs and gives each component/program complete autonomy to make their own decisions 2) Relies on accepted and evolving federation standards including SAML, Liberty Alliance, and WS-* 3) Is consistent with GSA's eAuthentication initiative 4) Is likely to be the preferred approach for inter-agency communications	1) Does little to meet the short-term (2005) needs of DHS, and does nothing for programs such as US-VISIT and ODP. These programs would need to start from scratch to develop and implement functionality to support their needs 2) The DHS Technology Reference Model (TRM) would need to be extended to include multiple choices for directory, access management, and provisioning solutions, reducing its effectiveness for simplifying the infrastructure 3) Duplicate identity information will likely be stored within multiple repositories in the short term in lieu of federation, resulting in significantly more expensive deployment and licensing costs 4) Data synchronization between the multiple repositories will be very difficult to implement and achieve, increasing DHS' security exposure as the number of critical repositories continues to grow with time 5) It will be difficult for components and programs to establish Trust Relationships and meet the requirements for Level 3 or Level 4 authentication assurance until the smart card and/or MaxHR initiatives are deployed or a DHS-wide Certificate Authority is deployed that is cross-certified with the Federal PKI bridge. At that point, each component and program will need to build its own interfaces to these repositories to synchronize data with established authoritative sources in order to minimize security exposures and data quality issues 6) Federation technologies are continuing to evolve, which will force each component and program to continually upgrade its federation capabilities in concert with one another to keep pace 7) Comprehensive auditing that aggregates data from the various environments will be extremely expensive and difficult (if not impossible) to implement 8) DHS will not be able to centrally administer or enforce common security policies. Each component and program will be forced to implement security and access control requirements within its own environment 9) This approach is not conducive to combining various help desk environments into a single, more-centralized approach being promoted within the ITO

7.2 Alternative 2: Leverage Existing Components



Advantages	Disadvantages
1) Minimizes the number of repositories being deployed within DHS and synchronization requirements 2) Leverages the investment already being made in Microsoft and/or IBM technologies 3) Requires no changes to the DHS Technology Reference Model (TRM) 4) Can meet some immediate DHS needs before year-end 2005 5) Can still support future federation needs with other agencies	1) Current programs are limited in scope to meet their own requirements and were never intended to support enterprise-wide IdM needs 2) Existing schemas will need to be extended and directory hierarchies may have to be "re-structured" to support general-purpose enterprise needs, extending the current schedule of the CBP ACE and/or ITO AD programs 3) If Microsoft Active Directory is leveraged, other vendors' access management and provisioning products will still be required for SSO, password management, and auditing capabilities

7.3 Alternative 3: Optimized IdM Solution



Advantages	Disadvantages
1) Technologies can be shared by multiple components and programs, simplifying the overall infrastructure 2) Consistent with Infrastructure Transformation Office (ITO) help desk consolidation efforts 3) Can meet some immediate DHS needs before year-end 2005 specifically targeted at eMerge2, US-VISIT, ICE, and ODP, eliminating the need for these programs and components to deploy their own solutions 4) Scales to support millions of users 5) Will meet future provisioning and federation needs by leveraging the process improvements defined as part of the smart card program and MaxHR initiative 6) Supports both centralized and delegated administration of users AND policies (both DHS-wide and organization-specific policies) 7) Simplifies integration with other critical repositories 8) General services could be "tailored" to meet the specific needs of individual components and programs	1) Requires deploying yet another directory instance or instances 2) May require changes to the DHS Technology Reference Model (TRM) 3) Default schemas will still need to be extended to support general-purpose enterprise needs 4) Forces components and programs to think globally and use centralized services, compromising the "autonomy" they currently enjoy to make their own decisions

8 Project

Pending approval and funding, the most immediate needs for the DHS IdM project going forward include:

1) Establishing an IdM governance board consisting of additional analysts, business representatives, and technologists from various DHS components and programs that will:
    a. investigate component-specific or program-specific processes for managing identities,
    b. develop a more cohesive enterprise-wide set of processes for on-boarding and terminating contractors,
    c. identify DHS wide UID standards, and determine authoritative sources and required data flows to/from other critical DHS repositories.
2) Selecting a limited set of DHS components and programs for the initial deployment
3) Assigning business analysts from various components and programs to determine the detailed short-term and long-term requirements for each participating components and programs.
4) Acquiring vendor solutions and systems integration specialists to deploy the necessary technologies in a phased manner,.

8.1 Period of Performance

The preferred timeline establishes partial initial operating capability in first-quarter FY06 and follows with full operational capability in late FY06 or FY07.

8.2 Summary of Work and Deliverables

The most immediate needs include the directory infrastructure, the centralized access request system, and necessary delegated administration tools. A preliminary work breakdown structure for standing up IdM is identified below.

Activity	**Summary Description**
0. IdM Project	
1.1. IdM Planning	Activities to mitigate risk, increase effectiveness, and increase the utilization of the shared Identity Management services. These steps do not focus on the technology; but focus on the activities that must be completed prior to developing the "enterprise" solution. Realizing many activities are already ongoing today, it critical to complete these tasks so that DHS is working from a common set of processes, plans, and definitions going forward.
1.1.1. Obtain approval for a formal	a) Confirm the requirements with stakeholder

Department-wide Identity Management Program / Initiative within DHS	organizations, develop and deliver an RFI to send out to potential vendors/integrators, and evaluate responses b) Develop a detailed project plan for implementing Phase 1 of the overall architecture c) Finalize the communications plan. The communications plan should include an abbreviated vision and strategy for the IdM program. It should also be a vehicle to inform stakeholders, users, and influencers of the end-state solution. Finally, it should allow for a two-way dialogue (both top down and bottom up) throughout the engagement.
1.1.2. Examine current and future budgets for IdM related initiatives and develop a consolidation plan	a) Identify current activities -- in whatever stage of maturity -- that can be transitioned into an enterprise service b) Look to develop a new budget that explains the changes in strategy along with impacts to existing budgets
1.1.3. Develop an Identity Management stakeholders organizational chart that outlines each program / component with a vested interest	The chart should identify points of contact for each program / component and a brief description of why they have been identified as a stakeholder.
1.1.4 Finalize requirements	a) Analyze the detailed requirements with representatives from each of the stakeholder organizations b) Finalize requirements for participating programs/components c) Determine enterprise requirements (common) and separate from program / component specific requirements d) Update requirements matrices and cite both a description and the source of the requirement
1.1.5. Complete Business Process Analysis	a) Document the current business processes surrounding the management of user identities and the establishment of accesses and privileges. b) This document must assess the impact to existing processes and re-engineered processes required for moving forward with an enterprise identity management solution. c) New business processes should be documented and accepted by the stakeholders prior to beginning development.

	d) Processes will need to change as the smart card and HR initiatives are rolled out
2.0. Establish Foundational Directory Infrastructure	a) Establish a sound foundational directory infrastructure that contains quality data and is well integrated with other critical repositories. b) General activities should proceed as soon as funding is obtained and will continue for 3-6 months depending on resources
2.1. Address governance issues and naming standards	a) Develop detailed schemas and data flows for the new general purpose directory environments b) Efforts should be complementary to and rely on new HSPD-12 compliant processes for quality data
2.2. Intranet Directory	a) Deploy and populate Intranet directory instance
2.3. Extranet Directory	a) Deploy Extranet directory instance b) The EXTRANET directory could be initially populated automatically with identity data from other Component/Program specific databases. c) Efforts should also identify detailed requirements for DHS-wide external user registration processes that meet DHS security requirements and can be consistently applied to various DHS Components and Programs.
2.4. Metadirectory	a) Develop meta-directory connectors synchronizing the INTRANET directory data with the Smart Card, MaxHR, Active Directory, web services, and other potential repositories b) Implement virtual directory capabilities
3.0. Implement User Administration, Policy Administration, Access Management and SSO Features	Establish foundational capabilities for UA, Policy, and SSO.
3.1. Single Sign-On (SSO) and Registration	Efforts should be focused on implementing the SSO features, the DHS-wide registration processes for users (using the self-service registration and approval features of the selected WAM solution), and access management/ policy mechanisms that meet the needs of current initiatives
3.2. Self-Service Registration	a) Self-service registration and embedded workflow approval capabilities will likely be required for both internal and external users who require a DHS "sponsor". b) A centralized access request system should be

	deployed where a user can fill out a form to request access, then have the form forwarded to their manager or DHS sponsor for approval. This central access request system can then keep track of all the accounts and system access privileges assigned to a particular user, and can then rely on other backend manual or automated procedures to actually create the necessary accounts. c) Delegated administration tools should also be delivered to authorized administrators or application owners within DHS components or programs so they can control who has access to their application(s) via groups and/or roles. d) Role engineering and more effective enterprise-wide on-boarding and termination process reengineering are also deliverables.
4.0. Implement More Robust Provisioning, Audit, and Password Management Capabilities	(Re)evaluate the Provisioning marketplace and product alternatives, and select an automated provisioning vendor or systems integration partner to implement extensive auditing capabilities, password management capabilities, and more robust automated provisioning solutions to improve upon basic access request-based features provided.