**Organization of the Technical Standards and Policies**

In order to achieve its goals, DHS is developing an information architecture, which will leverage the principles defined for the older technologies, and integrate the older technologies with new technologies. Standardized methodologies will successfully combine these different technologies.

DHS has organized all its technical standards and polices, and this document, into thirteen primary technical domains. These domains are Business, Privacy, Security, Network, Access, Knowledge Management, Platform, Integration and Middleware, Data, Operations and Support, Groupware, Applications Methodology, and ComponentWare. This document organization provides a structure in which to provide standards, policies, guidelines, examples and best practices, tools, and templates developed within DHS for its computer and information systems. The figure below presents the logical relationship and dependencies between the technical domains. Following this diagram are details about each domain.

**Organization of the Thirteen Technical Domains**

**Business Domain -** This domain provides guidance necessary for Department of Human Services (DHS) to become inherently better at managing programs by incorporating program and project management discipline into DHS's corporate culture. Ensure all departmental Information Technology (IT) projects are appropriately managed to provide reasonable assurance that projects have the highest probability of success. Support DHS executive leadership, senior program office management, and project teams by contributing advanced technical knowledge of complex system operations. Coordinate activities in the following key Program Management (PM) areas: PM Processes, Tools and Metrics; constant PM process improvement; Project Performance Assessment; Project Planning; Resource Planning; IT Standards Management; Business Process Re-engineering; Status Reporting; Project Communications; Contract & Vendor Management; Project Coordination; Quality Management; Financial Management; and Customer Support.

**Privacy Domain -** Addresses the privacy concerns of citizens and agencies with well-defined roles, policies, procedures and technologies. In addition, the Privacy domain addresses all state and federal laws related to privacy issues such as the distribution, availability, notification or permission to distribute and privacy violation notification. The privacy discipline focuses on the prevention of unauthorized viewing and/or acquisition of information about a person, case, or other classified activity.

**Security Domain -** The primary concern of an "open" architecture is secure access to the resources, including the data, for all end users in an organization. High access demands via the Internet make security issues particularly important. They need to address how resources are managed, how information is accessed, processed, and shared, how applications are developed, how Local Area Networks and Wide Area Networks are configured, and which tools are selected to manage those resources. Yet, security must still provide the "open" access that is required.

**Network Domain -** this domain specifies how information processing resources are organized, the protocols used for network communications, and the topology that shows how the devices are connected and physically wired together. The infrastructure consists of a series of Local Area Networks (LAN) connected together on a Wide Area Network (WAN). This topology allows for the seamless integration between, and centralized administration of, all of the devices within that organization. DHS has designed this network to provide a wide range of applications and resources, high reliability, scalability, support for new technologies such as voice, video, and voice over IP, hardware connections that are transparent to the end user, and affordability. All types of users must be considered, including remote users, and users with special needs. The network has built-in fault tolerance, is centrally managed. Modeling helps ensure that the network bandwidth is sufficient and built using industry standards and guidelines. Finally, the network is isolated from applications, seeks to minimize traffic during peak access times, and is designed considering middleware deployed.

**Knowledge Management -** this domain provides standardized techniques and procedures regarding codifying, storing, and retrieving data throughout DHS. Primary topics covered in this section include DHS Data Warehouse, Metadata repository, and other electronic document formats. The goals of the policies in this domain are to increase productivity and bring about a higher quality of service by providing a de facto standard for accessing and maintaining DHS's information.

**Access Domain -** Defines the roles, policies, standards and technologies that provide the framework for the electronic delivery of information and services to every government agency, business or citizen as deemed permissible under privacy and other mandated regulation.

**Platform Domain -** this domain defines the various components that comprise the computing infrastructure at DHS and includes the client/server, operating systems, and desktop PCs supported. The types of platforms employed depend on the overall business requirements of DHS. With the trend toward n-tiered applications, the integration of the platforms becomes the paramount concern. The development of architectural standards is a critical activity that helps guarantee that these tiers interoperate seamlessly. The principles that govern the platform domain include having a unified management approach, a backup and recovery plan, a viable technology replacement plan, and the minimization of the number of known vendor products being used at DHS. The platform components support the business needs of DHS, reside in secure environments, use industry standard products, scale to the desired environment, and maintain fault tolerance.

**Integration and Middleware Domain -** this domain relates to software that supports interactions between the clients and the servers and includes messaging, transaction, security, synchronization, queue, event, inter/intra application communications, and resource management services. Middleware allows for increased flexibility and adaptability and provides for easier integration between the application and services. For example, Middleware will provide DHS with the ability to change database platforms, infrastructure, and applications with minimal impact to DHS's application systems. Integration between third party software is also simplified because more of these products are based upon, and interoperate with, published Middleware standards.

The integration and middleware domain can be comprised of the following tools, techniques, and components:

* **Message-oriented -** provides a means of sending and receiving messages across an enterprise and includes queuing, guaranteed delivery, and synchronous and asynchronous processing
* **Object Request Brokers -** provide a method for application components to communicate
* **Transaction Processing Monitors -** provide transaction integrity services that helps ensure that 1) a unit of work is completed or rolled back, 2) updates are committed correctly in multiple target databases, 3) database reconnection takes place in case of outage, and 4) work is balanced equally among multiple database servers
* **Enterprise Application Integration (EAI) tools -** package Middleware and data hiding capabilities into one product
* **Rule Engine Tools -** are used to process business rules, route documents, and access to objects
* **Intelligence Agent Tools -** automate the creation of tasks typically performed by users

One principle that governs the Integration and Middleware Domain is to use only a minimal number of industry-proven products. These products are selected before the application development tools, because of Integration and Middleware products affect application development tools. The Middleware provides a common interface around distributed applications, allow for a separation between the user interface and business logic, allow for shared components, conform to published security standards, and provide for scalability in the application developed. Lastly, a Middleware recovery plan protects all components from possible disasters.

**Data Domain -** this domain relates to the capture, verification, storage, security, and management of data assets so that they are accessible to a wide variety of end users and systems in DHS. The data lifecycle is a series of processes that describe the movement of that data through DHS. In the initial stage of the lifecycle, the data is captured and validated. It is subsequently stored, and then acted upon by an application or set of applications. During that time, the data is stored in a managed and secured environment. Once the data has gone beyond its useful life, it is retired, then archived or purged.

This domain consists of a series of data architecture components, interfaces, and processes for implementing and maintaining a cohesive data policy, which include:

* **Databases -** all databases are repositories of organized data or data that is accessed by a database management system. There are three types of databases - operational, text-based, and data warehouses. The operational databases help support administrative and functional components of DHS. Data warehouses contain data that helps support decision making and executive information systems. Text-based databases are repositories for non-relational structures, typically information that is stored in its original document format.
* **Data Access Services -** these types of services include data maintenance, ad hoc query and reporting, and batch reporting. The data maintenance service provides a means of capturing, validating, and storing data through online or batch processing. The Ad Hoc query and reporting services provide the ability to create business inquires against a data store, or they provide structured reports against that data. The batch reporting services allow routine and regularly scheduled report generation for specific audiences.
* **Data Types -** relate to the way data is stored and processed on a database. Valid data types include character, numeric, image, voice, video, and predefined user data known as objects and text.
* **Data Distribution Services -** these services distribute the data to a variety of locations, thus minimizing the impact to performance on a network within DHS. These services include 1) replication - the process of synchronizing data in multiple locations, typically to read-only data, 2) extraction - the process of copying a subset of data from source databases to target locations, and 3) mirroring - the creation of multiple copies of a database that are synchronized simultaneously.
* **Data Resource Management -** defines the facilities used to maintain and support databases. The administration facility provides the means for the creation, maintenance, support, backup and recovery, and archival processes. Another facility, the meta-data repository, defines the physical characteristics of how data is stored. The retirement facility describes the means for either archiving or purging data from a database. The security facility provides protection and access to data on a database by authorized individuals.

A variety of computing components support storage, management, and data integrity. These include meta-data repository tools, database management systems, data administration tools, data modeling tools, data distribution tools, and database development tools.

* **Meta-data Repository Tools -** provide the process for acquisition, maintenance, and access to meta-data - typically for a data warehouse initiative. The two key components of the database management systems tools are the online transaction processing database and the operational data store. Operational databases capture data used for administrative and functional requirements. An operational data store is a single consistent image of an organization's data.
* **Data Administration Tools -** support the maintenance of data on a database and include creation, maintenance, support, backup, recovery, and archival activities.
* **Data Modeling Tools -** support the database administrators in defining the data models necessary, at the proper level of abstraction, to later support creating the actual logical and physical database structure.
* **Data Distribution Tools -** support the replication, extraction, and mirroring of data.
* **Database Development Tools -** support the development efforts for building a database structure. These tools include editors, debuggers, analyzers, and integrity checkers, and create stored procedures, database triggers, and views.

The fundamental principles that govern the data domain include central management of databases, identification of data owners, segregation of database types, development of proper backup and recovery processes, and conforming to standards. When designing databases, Data Domain staffs consider the infrastructure when making decisions regarding capacity and volume. They establish referential integrity rules, define a data dictionary, keep database replication and extraction to a minimum, perform prototyping, and use COTS software (which is industry proven) when possible. There are separate databases for each environment.

**Operations Domain -** this domain provides the high-level framework for identifying the requirements for centrally managing, maintaining, and supporting all of the infrastructure resources for DHS. This domain also outlines the standards, guidelines, and tools used at all levels of the infrastructure. These principles allow DHS to provide the greatest level of availability of those resources, resulting in improved service to their clients. The infrastructure resources include the servers, routers, databases, applications, networks, and Internet components necessary to conduct the automated business functions of DHS.

This domain contains three distinct layers: availability, infrastructure services, and operations. The availability layer relates to various components of DHS Technology Architecture that need to work seamlessly together. The infrastructure services relate to the ability to maintain the various components that comprise that environment. The operations layer relates to those services that help ensure that DHS's environment remains operational.

The principles that help guide the selection of components that support the entire DHS infrastructure include:

* **Compatibility -** all components are compatible, provide standard configurations, and are centrally managed. This allows for expeditious problem resolution.
* **Simpler Configuration -** since components are interoperable, the configurations tend to be less complex. This leads to selection of a smaller subset of vendors to supply components.
* **Use of COTS -** has many advantages, as it decreases compatibility problems, provides a larger customer base for support, and allows for concentration on DHS's business requirements, rather than software installation and maintenance.
* **Use Reputable Vendors -** third party products from reputable vendors provide a greater level of stability. In addition, these vendors tend to conform to industry standards that further improve that stability.
* **Future Growth -** the components provide for DHS's current and future demands.
* **Recoverability -** continued service to clients is a paramount issue that needs addressed by a robust disaster recovery plan.
* **Total Cost of Ownership -** the components provide cost effective alternatives for ownership and replacement.
* **Project Management Tools -** provide effective methods for identifying, tracking, and resolving problems that arise in a production environment.
* **Transparent Technology -** the framework components do not hinder the definition and resolution of problems that may arise in DHS. In addition, the technology provides maximum scalability and allows a wider range of configurations.
* **Enterprise Management Tools -** provide adequate metrics and reports to help support the management of assets of DHS. These tools monitor customer service and each of the domains. Some of the areas that can be monitored include system capacity, availability, and stability.
* **Problem Routing -** the components have appropriate alert mechanisms that route the definitions of problems to the appropriate resources.
* **Remote Access and Management -** provides the ability to remotely access and manage the assets of a particular system or the full system that serves DHS.
* **Limited Customer View -** each customer focuses only on his or her own area of responsibility.
* **Asset Management -** DHS assets are maintained and current. The Operations Domain uses tools that help with those inventory activities.

In addition to the above mentioned domain principles, four component standards are part of the Operations Domain:

* **Network -** network protocols are based on the Simple Network Management Protocol (SNMP) standard
* **Monitoring -** the ability to monitor network performance and capacity is based on the Remote Monitoring (RMON) standard
* **Desktop -** the desktop components work seamlessly together, if they comply with the Desktop Management Interface (DMI) standard
* **Internet -** Internet applications are based on standards published in the Data Domain

**Groupware Domain -** defines the environment where information sharing occurs between people, between automated processes, and between both people and automated processes. This includes collaboration and communication between individuals within and outside of DHS's organization, through formal and informal exchanges of ideas, documents, and the like. This domain relates to the other domains by defining the tools used to access data, process unstructured data, manipulate agency data, and document the application. It also uses components of the Internet and the Network Domain and coordinates with the Security Domain.

**Application Domain -** this domain relates to the technologies, standards, and guidelines for the development of applications within DHS environments. These encompass traditional mainframe based, 2-tier and 3-tier client/server, and n-tier architectures. These application technologies can be further defined by their flexibility, robustness, end-user interaction with the developed applications, and how these applications interact with each other. Since all of the tiers in the n-tier approach are highly scalable, they provide the greatest degree of flexibility and performance.

The technology components of the application architecture domain include:

* **Application Tiers -** regardless of the technology used, all applications include three basic functional areas: business processes or rules, data access, and interface strategies and processes.
* **Application Components -** are the common objects used by the developers to build an application. This write-once-use-many time’s concept is critical in large-scale application development and implementation efforts.
* **Application Development Tools -** the tools used to build the application must allow for portability regardless of platform. The Application Domain selects development tools based on their robustness, the ability to address a particular technical component, or to generate application code. Typically, developers use a combination of these types of tools in the development and deployment of an application.
* **Application Support tools -** include software and documentation version control, distribution, testing tools, report writers, requirement definitions, and application security.

The fundamental principles outlined in the application architecture domain help ensure that the design employs open architecture concepts, adheres to outside standards, is simple, supports object-oriented principles of program reuse, considers DHS's security concerns, and uses documented and repeatable development strategies. Application design is partitioned across multiple tiers, allows for stress testing and user acceptance testing, and is platform independent.

**ComponentWare Domain -** this domain provides standardized criteria for efficient reuse of existing application assets to enable faster deployment of new applications. This domain will further assist object-oriented analysis and design. Such techniques will allow reuse of software components and enable systems to respond quickly to change. Therefore, with the constant advancement of computer technology, the effective reuse of software components will allow DHS to give exceptional client service.

Terms Used as Headings throughout the Document

Many subsections of this document contain the same five section headings. Each of these section headings indicates the type of documentation you will find under that heading. For example, you will find standards documentation under **the Standards** heading and Guidelines under the **Guidelines** heading.

The five section headings are **Standards, Guidelines, Examples and Best Practices, Tools, and Templates and Forms**. Following are definitions of each term (and phrase) used in the five section headings.

**Standard -** A standard is a specific rule, set of rules, or policy that must be followed. For example, COM Development Standards is a set of coding conventions used for application development using Microsoft Component (COM/COM+) architecture.

**Guideline -** A guideline is a recommendation. It is less binding than a standard in that it does not require compliance. For example, instructions on how to complete a certain template or form would be a guideline.

**Examples and Best Practices -** An example is either a template or form that has been completed, or a method that has been implemented. A best practice is an example proven in the industry as an effective method for achieving the solution. The examples and best practices provide useful research material for readers, encouraging them to use the best practices followed in the IT industry.

**Tool -** A tool is a specific software application or utility used in a specific area of technology. This document familiarizes the reader with the tools used at DHS today, and thus identifies which tool(s) the reader should use for a given task. For example, Cognos PowerPlay is the standard OLAP tool used in the DHS Data Warehouse. The reader must use Cognos PowerPlay as an OLAP tool.

**Templates and Forms -** A template or form is a skeleton used for requesting a certain service. For example, there is a form to gain DHS network access. Instructions to complete a template or form are located under the Guidelines section, if any exist.

For more information regarding this document contact William Torres at wtorres@pa.gov.