U. S. Department of Justice
Information Technology Strategic Plan

Appendix C

Infrastructure Strategy

White Paper

Appendix C
Infrastructure Strategy White Paper

Background

Infrastructure can be defined as the collection of information technology (IT) elements that provides the technical features and capabilities necessary to implement business functions. It encompasses the layering of technology capabilities from applications through telecommunications as shown in Figure 1. Specifically:

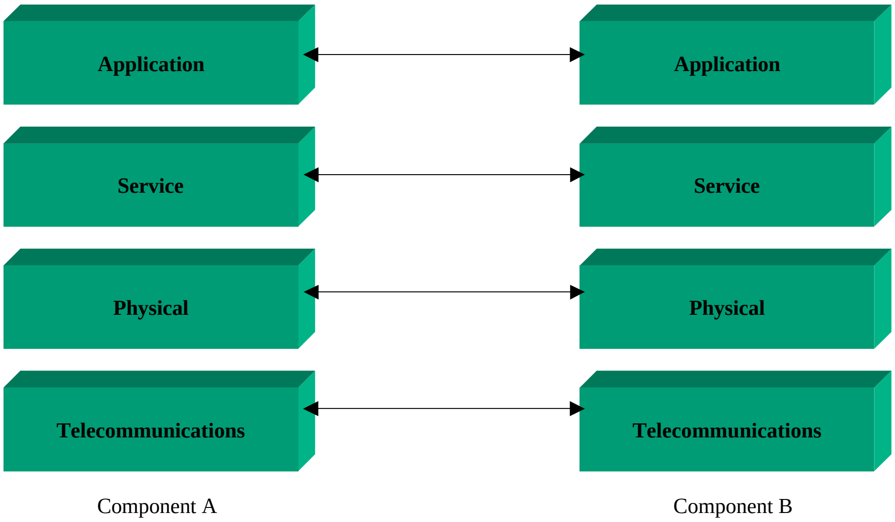

Figure 1

- The application infrastructure consists of the programs that implement and automate business functions. These may be either custom developed to provide a unique business capability or commercial-off-the-shelf to serve in a more general role.

- The service infrastructure consists of intermediate and often general-purpose services upon which applications may be built. This infrastructure layer includes components like programming languages, electronic mail transport systems and user authentication services. The service infrastructure is build from physical infrastructure elements.

- The physical infrastructure consists of the commercial products used as building blocks for the services infrastructure. They include computers, software packages, cables and other tangible products that are assembled to build the more complex service infrastructure.

- The telecommunications infrastructure provides connectivity between upper infrastructure layers. It consists of the wide and local area networks as well as wireless data, land mobile radio and plain old telephone service (POTS).

The Department uses numerous large and small IT systems to support its missions and objectives. These IT systems provide the computing infrastructure with which the business processes of the Department are automated. The infrastructure components are usually owned and operated by the various Justice organizations that use them, with a few exceptions. For example, wide area telecommunications data infrastructure is often leased.

JMD operates two central data centers that consolidate computing functions. The JMD data centers provide a centrally operated and managed computing resource exhibiting high availability through the use of mainframe computers maintained by a 7 by 24 staff (i.e., 24 hours day, 7 days a week). As IT evolves, the mainframes are giving way to farms of UNIX and Windows servers. Located in Rockville MD and Dallas TX the two data centers provide geographic diversity with the goals of providing mutual backup capabilities (high availability) and computing resource consolidation (cost containment). In actuality, the two centers lack the redundant telecommunications needed to support a seamless fail over from one to the other in the event of a critical failure of either. Additionally, the two centers provide only a limited subset of common computing services resulting in a limited and highly manual fail over process. There are computing resources located at component locations across the nation as well. Although, redundancy exists in some systems to support fail over, there are no Departmental standards for availability or survivability of the IT infrastructure. Each component must provide contingency planning as part of the certification and acceptance process but the plans many times do not always provide for reasonable IT continuation during the loss of critical IT infrastructure.

The Department has implemented office productivity desktop services through the Justice Consolidated Office Network (JCON). It consists of standard desktop software and centralized electronic mail, file storage and help desk services. JCON consolidates and standardized desktop capabilities to a significant degree. Still, JCON installations can be tailored to meet individual component needs, thus diluting the intent and leverage of a standard desktop. For example, both Microsoft Office and Corel Perfect Office are available to desktop users. Although there are somewhat compatible data formats in common to the two packages, many times information exchanges between users are cumbersome – document formats do not convert well from one product to another. JCON operates on the individual component's local area network (LANs) under a wide range of performance parameters, security conditions, and trust relationships. Also, JCON usage is not mandatory for the components. In particular the largest components have pursued their own unique solutions to providing desktop applications resulting in unacceptable interoperability among desktop users.

One of the biggest problems with the current IT infrastructure is the Department lacks an overall policy on how engineering decisions should be made to permit interoperability across the enterprise. Currently, the Enterprise Architecture exists as highly independent and fragmented component architectures. Each component has developed IT systems and solutions with only secondary regard for the enterprise. Interoperability is typically engineered on a per system, per mission basis without Department wide standards or interoperability guidance. This fact often makes unplanned interoperability a major undertaking for each new requirement and can force crisis development and deployment efforts to establish new interoperability when urgent events arise.

The Department performs many diverse business functions ranging from financial management, law enforcement and litigation, among others. Each of these functional areas has supporting applications operating in a legacy infrastructure environment consisting of "stovepipe" systems and data supporting unique business functions. Some server consolidation has occurred; mainframe computers host applications from several mission areas. However, to date, the Department lacks an overall plan for developing applications and systems with respect to the complete enterprise, resulting in disparate islands of IT infrastructure within each component. Each component, being focused only on their specific missions, has developed systems and applications without a view of the Department enterprise resulting in a plethora of overlapping and non-interoperable applications and databases.

The services infrastructure suffers from the same silo approach that impacts application interoperability. Systems like electronic mail have limited usefulness because the implementers approached it as a communication tool to be used within the component rather than throughout the Department. This has resulted in the use of several different email systems that provide only the most basic interoperability and restricts, to the component's domain, many advanced features (e.g. calendaring and public folders) desired by the users at an enterprise level. Other services have been implemented using similar narrowly focused approaches, resulting in systems that often work very well within a component, but do not interoperate well at the Departmental level.

The physical infrastructure is varied and diverse. Each component has selected products to implement its infrastructure with little Departmental guidance. The various component data centers operate a wide range of hardware and software. The use of features unique to a specific vendor limits the portability of applications and services.

Efforts to consolidate the telecommunications infrastructure have had mixed success. Although the Justice Consolidated Network bundles and resells bandwidth based on standard protocols, it has failed to gain critical mass, where the projected cost savings have been realized. There are still large numbers of dedicated leased point-to-point circuits in use throughout the Department.

Vision

The Department requires seamless interoperability between IT systems. This goal can be met with a unified IT infrastructure. A unified infrastructure specifies horizontal and vertical interoperability guidance for each of the infrastructure layers shown in Figure 1. This goal must be met within the context of affordability. The following features outline a vision and direction for the Department's computing infrastructure that will satisfy current and future business needs.

Information Exchange – With a unified infrastructure, interoperability will provide users access to the right information at the right time. To meet the Department's data sharing goals, authoritative databases must be available to appropriate users needing the information they contain from anywhere within the enterprise. Fundamental to meeting the goal of data sharing is information protection and security. Users must be authenticated and exhibit the need to know before being granted access to critical Department data. Technologies are evolving, particularly in the area of knowledge management, to allow subject matter experts to extend their reach throughout the enterprise. Data mining and other analysis tools provide users the ability to access and examine views of information of their own choosing. No longer will it be acceptable to require a programmer develop a unique application to provide a unique view of information, as this flexibility can be given directly to the user. Systems will be able to exchange information throughout the enterprise. Data definitions will be universal within the Department.

Flexibility and Adaptability – The unified infrastructure will respond to changes in requirements without requiring extensive changes to the infrastructure. Systems must exchange information on demand using universal data formats and exchange mechanisms. It is no longer acceptable to have multiple systems deployed that perform the same job. Standardization of applications across the Department will allow the use of systems that can serve a number of the components. Systems must be extensible to meet the unique requirements of specific components while allowing the maximum reuse of software, common to all components. Networking will become ubiquitous. It will no longer be necessary to engineer a communication path to support a new data exchange requirement or application.

Ubiquitous Computing - The unified infrastructure will allow Department users to access their systems from anywhere in the enterprise. The reach of enterprise computing will expand with the introduction of wireless data technologies and hand held computing platforms. Additionally, the deployment of secure integrated networks will provide the user access to the systems and applications they require to complete their jobs anywhere in the enterprise. This provides significant advantages for disaster recovery and contingency planning. With few exceptions, all Departmental workstations should support the execution of a common set of core Department applications developed around a common application reference architecture.

High Availability – The unified infrastructure can help meet the critical goals of high availability. As computing becomes more important to performing the Department's functions, it is critical that systems be available when needed. Redundancy in the infrastructure allows high availability by providing redundant communications and services upon which applications are built. Standardization of platforms and ubiquitous networking provides portability of applications.

Predictable Development – As the Department's applications become more complex and widespread, the acquisition and development processes become critical to meeting the Department's goals. This plan envisions planning via the Enterprise Architecture process. This planning will precede a unified acquisition and development process to support the introduction of infrastructure into the Department. This process shall use metrics and public reviews to inform the user community and program sponsors of the status of acquisition and development efforts. User involvement will occur at all stages of the acquisition and development process.

Strategy

The Department requires a unification of the infrastructure through the systematic modernization of the application, service, physical and telecommunications infrastructure layers. The Department must build infrastructure using an enterprise infrastructure architecture. Specifically this architecture must address.

- Interoperability – Applications, services and telecommunications should be based on an enterprise architecture implemented with technology and configuration standards to facilitated interoperability among component systems at all levels of the infrastructure. Interoperability should be general purpose and "matter of fact." Changes in missions should require no or minimal changes to the infrastructure.

- High Availability – High availability systems are those that have sufficient redundancy to resume mission operations after the failure of one critical component, after an acceptable fail over interval. High availability functions can be achieved through component redundancy and geographical diversity within a framework or process for fail over. Each business function along with its supporting mission critical application must be evaluated to determine availability requirements. These requirements will then be used to determine the degree of redundancy required and a suitable fail over process and strategy. Ubiquitous networks will allow the centralization of mission critical systems into a few high availability data centers, which can serve as mutual backups. The data centers will possess telecommunications diversity, redundant power and environmental systems, appropriate physical security and a trained staff of operators and technicians.

- Component Portability and Reuse – Software will be developed so that it can be reused to support like functions at different components. Software objects must be supported as libraries for reuse within multiple applications. Applications must be developed around a reference architecture to allow common or core capabilities to be developed once and shared by all systems needing the same functionality. The reference architecture must be extensible to allow adding component or mission specific software components to augment the capabilities of standard applications and libraries. All applications should share a common set of user interface (UI) characteristics and behavior.

- Enterprise Development - The Department must develop a business process for IT system acquisition and development. Formal processes for major and significant systems, incorporating public reviews, will provide management and users insight into the progress and effectiveness of the pending solutions pertaining to acquisition and development efforts. The overall process must address all areas of the system life cycle to include requirements definition, development or acquisition, operations, maintenance, testing, training, certification and acceptance, and end-of-life-disposal.

Recommendations

The following recommends are made:

1. Assemble a team to produce an enterprise infrastructure architecture. This team should be led by the JMD/IRM/IMSS Enterprise Architecture Group with participation from the components. This group will collaborate as a team in a sustained effort until the architecture is published.

2. Evaluate the current component infrastructure architectures for points of unification. Consider unifying email services, directory services, office automation and other easily identifiable compatibilities to determine the feasibility of implementing near term fixes to common problems.

3. Commence the development of a public key infrastructure (PKI) solution to address the security needs of the unified infrastructure. The unified infrastructure can create significant security vulnerabilities if not designed within the context of a comprehensive, integrated security architecture implemented with appropriate technologies. Federal agencies are beginning to deploy PKI. It appears that PKI can help meet the needs of the Department with respect to securing the IT infrastructure. Since a number of the components are beginning PKI deployment, this recommendation brings those projects together with the goal scaling these integrated initiatives to meet the PKI requirements of the Department.

4. Develop an Application Reference Architecture (EAG). This architectural component describes the mandatory interfaces, standards, and services to be used in the development of applications programs. Additionally it describes an application framework for software delivery and extensibility. Recommend the EAG commence identifying application segment architectures based on Departmental business areas.

5. Develop a list of approved technology products to address standardization of the physical infrastructure layer.