



SECTION 5

INFORMATION TECHNOLOGY ARCHITECTURE

1100011000079

INFORMATION TECHNOLOGY ARCHITECTURE

FEATURED IN THIS SECTION

- 5.1 Enterprise Architecture..... 1**
- 5.2 Application and Data Architecture 3**
 - 5.2.1 The Application Tools..... 4
- 5.3 Platform Architecture 5**
 - 5.3.1 Platforms..... 5
 - 5.3.2 Storage Area Network..... 5
- 5.4 Network Architecture 6**
 - 5.4.1 Enterprise Data Communications Network 7
 - 5.4.2 Institutional Network (I-Net)..... 8
 - 5.4.3 Mobile Data Network 9
 - 5.4.4 Voice Communications Network 10
 - 5.4.5 Public Service and Public Safety Radio Networks..... 10
- 5.5 Internet Architecture 10**
- 5.6 Security Architecture..... 12**
- 5.7 Technical Architecture..... 14**

SECTION 5

INFORMATION TECHNOLOGY ARCHITECTURE

5.1 Enterprise Architecture

This section identifies current information technology architecture implemented in Fairfax County. The county's technology architecture is a tactical asset that defines technology components necessary to support business operations and the infrastructure required for implementation of new technologies in response to the changing needs of government business. It is a multi-layered architecture that includes:

- Application and Data Architectures
- Platform Architecture
- Network Architecture
- Internet Architecture
- Security Architecture

Enterprise Architecture Process Model

Fairfax County adapted Enterprise Architecture (EA approach) as the blue print or roadmap by which specific technology solutions are developed. Architecture defines the manner in which technology is used to enable flexible business solutions which enable expansion and change as requirements evolve, technology is updated, or becomes obsolete. Architecture as a foundation and roadmap enables the county to establish open standards, assess the impact of new requirements and evolving technologies, and allow for the incorporation of new technologies as part of an updated blueprint that benefits

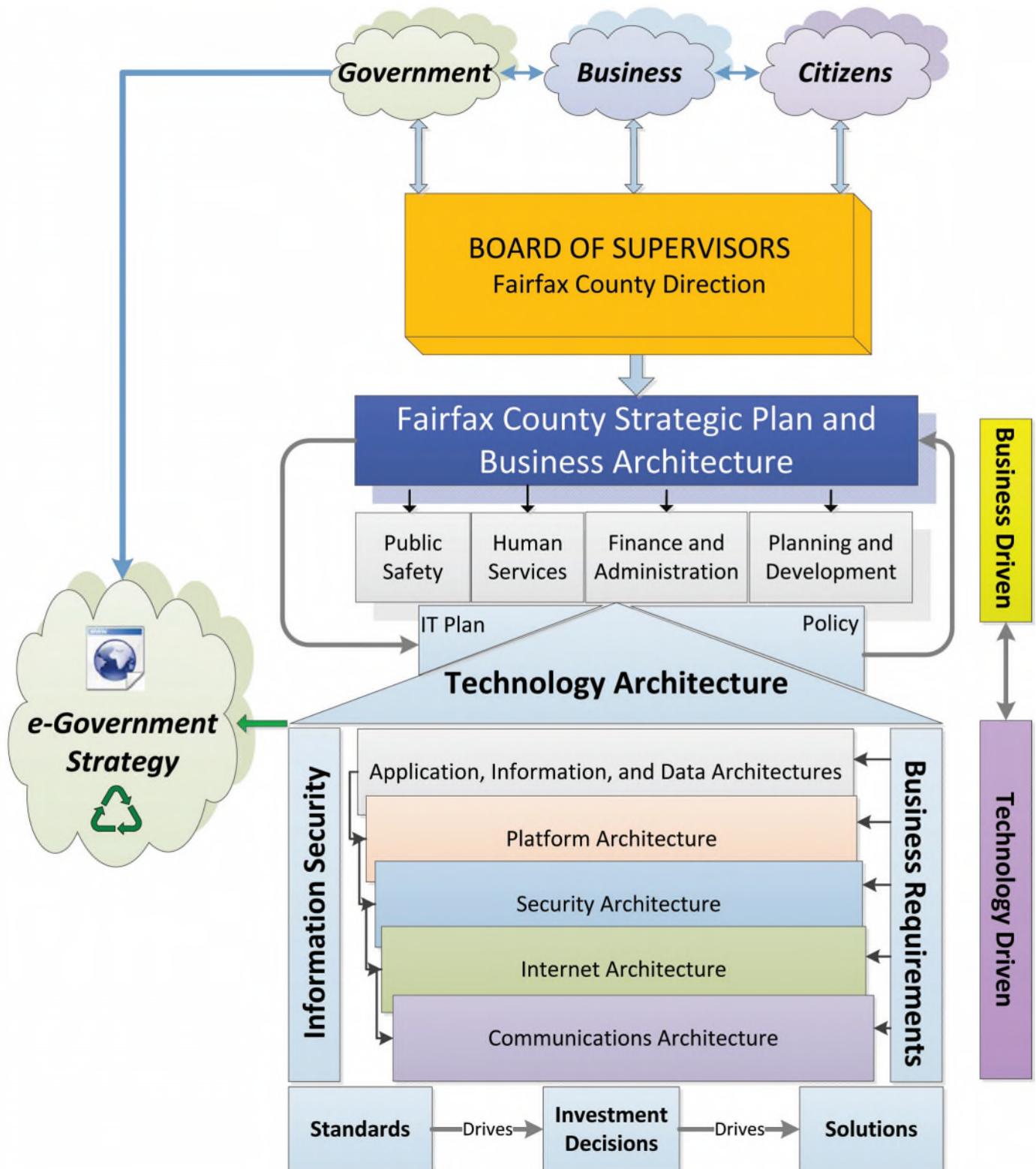
other solutions. Enterprise Architecture improves the efficiency and effectiveness of technology investments by reducing functional redundancy, leveraging solutions and platforms, optimizing value, and promoting the sharing of knowledge and best practices across county government.

The Enterprise IT Architecture Process Model on the following page illustrates the inter-relationships between the county's IT architecture and business, and the iterative processes involved to ensure the development of an IT enterprise that is efficient, cost-effective, responsive and business driven. For the purposes of the county's model, the businesses have been grouped into four major functional areas; Human Services (HS), Public Safety (PS), Planning and Development (PD), and Finance & Revenue (F&R), inclusive of over 50 departments and agencies representing hundreds of unique and often times cross-agency services.

The model is based on the following Mission Statement that directs the county's information technology activities. Every effort undertaken is framed and aligned with this mission statement:

"Delivery of quality and innovative information technology solutions for agencies and those doing business with Fairfax County Government."





5.2 Application and Data Architecture

Application architecture defines the design of and correlations among software programs and applications. The Architecture promotes common development and presentation standards, enables optimum system integration, provides opportunities for use of shared infrastructure environments, servers, storage and related tools, enables shared use of data, facilitates the reuse of components, and the rapid deployment of applications in response to changing business requirements. Application Architecture includes elements of technology architecture that converts business process to business intelligence to support the county's goal of delivering timely, efficient and cost effective services. In Fairfax County a vast inventory of enterprise-wide and agency specific applications reside on mainframe, server, cloud services, desktop and/or mobile computer platforms. New applications and application enhancements are constantly evaluated, developed or acquired, and applied as older "legacy" applications retire, or, business organizations and related functions reorganize and/or have new needs.

The county's goal is to use industry standard application development tools and language environments that are adaptive in web-enabled models. The Application architecture also protects the county's investment in 'classic' systems by enabling enhancements that enable enhanced usability, improved data analytics, search and reporting and end user controls. In addition, by keeping abreast of emerging technologies such as Web Services, XML, SOA and other contemporary methods, the county positions itself to take advantage of emerging opportunities offered by these as well as SaaS, mobile and cloud technologies. An exhaustive discussion is beyond the scope of this section; however, some examples of the county's application architecture and some recent developments are described here.

As the county balances determination among Commercial-Off-The-Shelf (COTS), in-house development and cloud/software subscription services for the diverse portfolio of agencies' business systems, the new framework for application development is applied. The framework incorporates Software Engineering, Information Architecture, and Application Development Methodology. These principles and techniques are used to keep the Systems Development Life Cycle Standards (SDLCS) current. The resulting approach encompasses application life cycles for "cradle to grave"; that is, from the earliest stages of planning,

through requirements and design, to implementation and post-implementation support, and hot back-up. New applications will be built on the most current and promising platforms and an architectural framework based on the future of IT taking into consideration industry best practices and sustainable trends.

Development platforms such as .Net and standards such as XML and Web Services are a key part of the strategy. The .Net platform provides the foundation for departmental and enterprise-wide applications and offers a stable application environment with more opportunity for componentization of business logic, sharing of common components, and the integration of business processes across application boundaries. Tools such as Visual Studio.Net provide county developers with a robust and flexible development environment. Encapsulating both existing and new business logic into "Web services" provide the ability to expose business processes across organizational and application boundaries, within the county, other local jurisdictions, state and federal government, as well as business partners. XML provides the common "glue" to hold together and provide consistent information across boundaries to facilitate data sharing among disparate platforms and systems. Enterprise Application Integration (EAI) products such as WebMethods and Microsoft BizTalk allow virtually unlimited ability to share, incorporate information and business process from older, mainframe and client/server applications in to the new environment. A detailed "Architectural Framework" document has been developed, and is intended to be an organic document, flexible enough to reflect and incorporate rapid advances in information technology.

Geographical Information System Applications (GIS) –

The ArcGIS software suite provides high-end geospatial technology, GIS tools and functionality and presentation to the GIS user community. The software integrates visual or graphic data in the form of maps, with descriptive or attribute information from an organization's internal databases. ArcGIS provides to tools for analysts to gain access, visualize, and query both graphic and tabular data for better analysis and decision-making. There are three levels of license usage for ArcGIS that the county uses. The highest level, ArcInfo, is used by professional GIS analysts for sophisticated analysis and processes. The View level is used by most users for map creating and simply analysis of the county's geographic data sets. Arc Internet Map Server (ARCIMS) and ArcGIS

Server are two components used to distribute highly customized GIS based applications through the Internet / Intranet. Internet based mapping capabilities are

incorporated as appropriate for augmenting and using available applications for public and internal government access via the WEB.

5.2.1 The Application Tools

Application tools are information technology components used to develop and support application functions. Application tools include the support systems required to enable work planning and communications.

Programming/Development Tools – New applications are currently under development using fourth generation object oriented languages and tools. This approach continues as web-based applications are developed, or as Commercial-Off-The-Shelf (COTS) systems or Cloud and SAAS applications are implemented. Industry standard life-cycle methodologies are employed to define, develop and implement new systems. Expert system technology is used to incorporate complex rule based functionality into systems. New developments use ASP and ASP.NET for the application layer. The county uses webMethods and Microsoft BizTalk to help with the integration of applications at the presentation, business logic, and data layers. Documentum is the county's enterprise content and document management software solution standard. The county also supports REAMS imaging solution.

Since often times there are no viable COTS or SaaS available that meet county agencies' unique governmental business needs, software development remains relevant, thus Software Engineering technologies are incorporated into the Systems Development Life Cycle Standards (SDLCS) to provide a disciplined and consistent development approach.

Collaboration Tools – The county uses Microsoft SharePoint and Office Communication Suite which includes instant messaging and web conferencing. Additionally, the county uses other video conferencing and web conferencing tools to support collaborative communications. ThinkTank is used for Group session Collaborative Software for Group Decision Support. Groups use the computer-supported meeting center software to conduct process improvements, strategic planning, program evaluation, and vendor selection sessions.

Database Management Systems (DBMS) – The county uses several database management platforms to support

its business applications. Oracle and Microsoft SQL Server are the county's databases standards. Currently most of the Oracle and SQL databases on standard COTS development architectures are consolidated for greater cost efficiency, supportability and performance. The county IT standards call for complex, Internet-accessible or high access databases to use Microsoft SQL Server or Oracle, as appropriate. However, there are also "fat client" and web-based agency specific applications that are maintained separately by agencies. Most of small agency applications use Microsoft Access or Microsoft SQL Server as the database and programming language architecture.

Enterprise Decision Support Systems and Business Intelligence – The county's portfolio currently contains several products used for reporting, analytic, and decision support. Business Objects / Crystal Reports, SAS, QMF, SQL Reporting Services are the currently-supported tools for enterprise reporting, basic ad-hoc query, and departmental reporting. Many of these products were acquired through COTS solutions with embedded tools. The proliferation of tools and the associated support, training, and infrastructure costs present a strong business case for rationalizing the portfolio, consolidation and virtualization. SAP-BOBJ will provide reporting and BI across the enterprise ERP applications. The county's strategy is to provide shared enterprise capability and infrastructure for reporting, query, transparency and decision support. As standards are defined for the county's enterprise solution(s), the portfolio will be rationalized into fewer products over time. This approach enables DIT to continue to modernize the existing systems portfolio while creating economies of scale for improved interoperability, search, and cost control.

Desktop Office Automation/Workstation Software – Microsoft's E-mail and Office Suite is the standard for general productivity automation functions including Word, Excel, PowerPoint, Outlook and SharePoint. Microsoft Internet Explorer is the standard for Web browsing, implemented in the standard image. Microsoft Project and Visio are available via enterprise software provisioning or virtualized Citrix application delivery.

Agencies may have other desktop-based software for special, unique requirements.

IT Service Desk Software – The IT Service Desk provides county employees centralized portal for computer support. InfraEnterprise (BMS) is the web-based solution

used to support the Service Desk function leveraging the ITIL framework. The Automatic Call Distribution (ACD) capability on the Avaya voice system is used to route calls. The IT Help Desk has a high percentage of first-call resolution.

5.3 Platform Architecture

Platform architecture defines the technical components of the infrastructure including server and client platforms, middleware, operating systems and interfaces supported, as well as other software tools and equipment used to operate applications. With the county's server consolidation and virtualization effort in FY 2011, Fairfax County's platform architecture was reduced from over 1000 servers to an average target ratio of 60:1, a project that continues into FY 2013. Servers include UNIX (Sun Solaris) and HP UX, Microsoft Windows /2008, 2008R2 and z/OS mainframe. Over 14,000 PC's provide end-user

access to county systems. Laptops, iPads, Blackberries, iPhones, Droids, and other tablets and mobile devices also support employee access to agency business systems. Workstations are standardized using Windows 7 operating system. The total data storage requirement has grown from 394 gigabytes in 1998 to the current total of over 1.3 petabytes. The county supports over 1,000 State and other non-county Windows workstations hardware devices. The following paragraphs describe the major features of the county's platform architecture.

5.3.1 Platforms

Desktop PCs, workstations and Peripherals – DIT prescribes hardware platforms and desktop applications standards as well as procurement vehicles to optimize support and cost. Workstations (PCs) are replaced in accordance with the county's PC Replacement Program cycle using adopted standards bundled with the MSOffice Suite. The PC Replacement strategy applies to all agencies and provides the county economies of scale as well as a more robust, effective support environment.

County PCs are used for office productivity software, enterprise e-mail and client software, Internet/Web access software, and mainframe emulation terminals. Windows 7 and Windows Mobile, iPads, Droids are currently being deployed. Windows 8 will be deployed in 2013-14.

Desktop and network printing is accomplished primarily through the county's enterprise multi-function copier/

printer/scan/fax machine fleet. Agencies also use stand-alone desktop or work-group printers, and special use machines, i.e., plotters, etc.

LAN-based Network Servers – Fairfax County's enterprise server environment uses Intel and Unix-based servers. Enterprise-class server technology (e.g. UniSys ES 7000, DELL/IBM Blades, SUN and HP-UX servers for robust, high availability applications) support the county's enterprise infrastructure applications such as Exchange, Active Directory, SQL, Oracle, Citrix, and major business systems such as ERP, GIS, Tax systems, Human Services systems, Land Development and Public Works applications, Library, etc.

The county has standardized on VMWare for virtualization platform and consolidated over 800 servers to the virtual environment. Virtualization in the SUN/Solaris environment in form zones has been implemented.

5.3.2 Storage Area Network

Fairfax County implemented its first Storage Area Network (SAN) in 2002. This enabled data storage in a centralized location, with redundancy and failover, mitigating the risk of data loss due to hardware failure. Data from all servers (mainframe, UNIX, and INTEL) now

coexist on the same disk subsystem. In 2006, the county refreshed the enterprise disk arrays and fabric with EMC DMX-3 disks and Cisco fabric. The county recently enhanced storage by implementing NetApp and IBM XIV storage systems, which positions the county for

future growth and the ability to meet strategic initiatives for Data Lifecycle Management.

Storage Management requirements addressed by the SAN are:

- Scalable storage capacity that allows users to increase storage as needed.
- Modular, adaptive architectures which allow users to deploy storage in a variety of centralized and distributed environments with re-deployment capabilities as needed.
- Highly available architectures to minimize/prevent downtime.
- The storage solutions provide a range of cost savings. Using NetApps for virtualization standard storage platform saves the county money because of the built in features such as de-duplication, which help to control the amount of storage needed for the counties growing server requirements.
- The new XIV storage provides the high volume input/output operations required by our high volume Database and Email systems
- Higher levels of performance to support the ever-growing volume of online data.
- Higher performance backup and restore operations using snapshot technology helps to support shrinking backup windows
- The ability to share data across the enterprise rather than building "islands of data."
- Easy to use, centralized management tools that allow hardware and data to be distributed.



5.4 Network Architecture

The county views a strong, viable communications infrastructure as a vital component to the overall IT strategy of maintaining its successful deployment of cost-effective solutions that optimize business goals. The enterprise communications infrastructure includes voice and data technologies, as well as various network topologies, transmission services and protocols necessary to facilitate the interconnection of server platforms, intra-building and office networks (LANs),

and inter-building and campus networks (WANs). The network is thus responsive and reliable for county business applications and allows for the uninterrupted flow of voice, data, and video information.

The plan and architecture take into account growth based on the needs of county agencies as programs expand for both intra and inter county connectivity. The core network for intra-county is supported by the

county's fiber I-Net, integrated with carrier lines for full coverage, back-up and redundancy for certain critical systems. The underlying infrastructure is able to support voice, data, and video, providing increased, cost-effective bandwidth potential, and improved output. The core fiber I-Net is a metropolitan fiber ring that connects over 400 county and schools facilities, with DIT supporting over 14,000 data ports and over 15,000 voice ports on the communications infrastructure.

Network technologies tend to refresh every 18-24 months, which creates additional challenges with respect to keeping network architecture and standards in

line with evolving business requirements, information security and other support needs. Web-enabled applications and Internet tools such as Social Media have rapidly expanded; this coupled with business continuity have resulted in expansion from a single high capacity DS-3 for internet services to four high speed LAN based Internet connections from two diverse IPS. E-Government applications, streaming video, teleconferencing, and more integrated and complex applications drive the requirements for the county's communication infrastructure and its components, thus the communications infrastructure is flexible and designed for low-cost, incremental enhancement.

5.4.1 Enterprise Data Communications Network

The Fairfax County Government's Enterprise Data Communications Network serves as the data communications backbone that provides countywide access to information technology resources. All systems connected on the enterprise network are based on well-recognized, open standards; compliance with published standards is required for any network-connected device or system. The county standard network protocol is TCP/IP. Gigabit Ethernet is the standard LAN backbone speed in the county and 100 MBPS is the standard desktop speed. All platforms are interconnected via the enterprise network including PCs, servers, multi-function printer/scanner/copier device fleet, and the mainframe computer. Additionally, various wireless technologies are rapidly expanding throughout the county's network. The county currently uses commercial broadband wireless infrastructure to support wireless applications, data, images, live video to the field and mobile devices supporting primarily public safety responders. The ongoing strategy has allowed for the integration of the wireless and wire-line networks.

The Enterprise Wide Area Network (WAN) is built of two different architectures: I-Net or the Institutional Network, which utilizes the dark fiber provided to the county through the COX and Comcast Cable Franchise Agreements (see section 5.4.2 below). I-Net spans seven hub sites and two key resource centers, Massey Public Safety Campus and the Government Center. These sites are networked via a 10 gigabit DWDM fiber optic backbone. The I-Net DWDM backbone provides connectivity to 192 remote sites running a 1 Gigabit uplink from the backbone to the site. I-Net also employs MPLS (Multiprotocol Label Switching)/VRF (VPN Routing & Forwarding) to allow I-Net to service many types of

diverse traffic whether it is enterprise, public access, public safety, or voice over IP. Through MPLS/VRF each type of traffic can be separated logically for security support, as in enterprise vs. public access, or prioritized in the case of voice traffic. Currently MPLS technology has allowed the county to support 20+ logical networks to flow across the I-Net backbone. I-Net has now positioned the county Data Communications Network to respond quickly to the ever-changing technology needs of its customers. The remaining WAN sites are supported by the use of several technologies to include High-speed broadband VPN technology, ATM, and Transparent LAN Services based on user group and bandwidth needs.

A dedicated Public Access Network was established in FY 2005. This network provides public access computers at various county locations to citizens of Fairfax County for access to county and Internet resources separate from the government Enterprise Network for security reasons. The Public Access Network includes all public libraries, community and recreation services sites, and select human services sites. The design provides for separate physical networks at each site while sharing the existing WAN/I-Net infrastructure and using logical separation on the WAN/I-Net. A firewall between the Enterprise Network and Public Access Network allows for county IT staff to manage the infrastructure down to the desktop for each site. This model will be the standard for any new facilities requiring both enterprise and public access.

The county continues to implement wireless LANs and wireless data over commercial systems as required by business and operational requirements. The use of this technology is carefully evaluated to ensure all county data is protected from unauthorized access. Currently,

can also serve as the back-haul for the county's wireless broadband initiative for public safety (See section 5.4.3).

The I-Net Video Network is a scalable integrated video transport system which provides a high quality image delivery system with scalable bandwidth, capacity, and growth potential for future Fairfax County Government and Fairfax County Public School applications. The I-Net video network transport has two distinct communication

links: Coarse Wave Division Multiplexing (CWDM) is the transport technology that provides forward and reverse transport for I-Net enabled county facilities. The forward (downstream) transport provides select cable TV operator channels and local origination content produced by the county's Video Production facilities for services such as distance learning. Each I-Net enabled facility is equipped to transmit reverse (upstream) video to the county's Video production facility for processing.

5.4.3 Mobile Data Network



To support operations of the various public safety agencies, the county activated AT&T and Verizon Commercial Wireless Broadband service in 2007 to allow the response vehicles of the Police, Fire and Rescue, and Sheriff's departments to access the county's Computer-Aided Dispatch (CAD) system, the Law Enforcement Incident Management system, and various databases maintained by the Commonwealth of Virginia and Federal law enforcement. This Public Safety system consists of more than 1500 Mobile computers Terminals (MCT). Both carriers are used to support a growing portfolio of mobile applications including Public Works and Environmental Services, Zoning, Health Department, and various Human Services agencies consisting of a user base of 750+ mobile devices.

Like a growing number of major local governments, the county applied for a FCC Waiver for use of 700 MHz for Public Safety broadband. The broadband wireless design is part of the comprehensive enterprise network strategy that will leverage existing voice wireless infrastructure (see 5.4.2.1), and integrate with the county's fiber backbone infrastructure for back-haul (see 5.4.1.2 below). The county has been vociferous in its response to the FCC, regarding the need for a private broadband wireless network for public safety for the National Capitol Region. Unfortunately, our waiver languished in FCC with no decision being made, and now with FCC's recent approval to allocate the D-Block 700 MHz frequencies to public Safety and first responders, and the creation of a board to manage and oversee this development, all pending waivers, including ours, were terminated until the new "board" takes effect and reviews the approach to a nationwide network. The county continues to accelerate its efforts, and is currently evaluating responses to an RFP for a vendor so assist the county to build a Public Safety Private Wireless Broadband Network using the D-Block allocation.

To enhance the county's goals for mobility, telework, operational cost efficiency, Continuity of Operations Planning, and environmental stewardship and 'green' IT, a major component of the enterprise technology infrastructure includes Enterprise mobile device management (MDM) that has been incorporated into the enterprise network and platform enabling infrastructure. MDM allow smart-phones, and tablets to include Apple, Blackberry, and Android (for example). With the county having a mature 'private' enterprise cloud, this technology has been adopted and being implemented integrated with the enterprise network. Symantecs Mobile Management Suite for the MDM architecture.

5.4.4 Voice Communications Network

The county's voice telecommunications architecture is the Avaya enterprise-wide VoIP capable platform. The solution uses the latest technology that includes VoIP and the county's fiber-optic network for connecting county facilities. Using the county's fiber backbone (I-Net) greatly reduces the total costs of providing telecommunications services. The evolution of the Avaya communications platform on a fully integrated broadband network synchronizes and leverages communications capabilities, security and will help meet the present and future IT and county agencies' business needs to complement cost saving advantage of using the I-Net for calls between locations, DIT is implementing Session Initiation Protocol (SIP) Trunking to further reduce the cost of the connection to the carrier network. This will ultimately lead to an end-to-end IP based broadband communications environment that is flexible, secure and very cost effective.

The voice system design uses two main Fairfax County government sites – the Massey Campus and the

Government Center Campus - as the "core" for the Avaya enterprise platform. A streamlined dialing plan has enabled more efficiency and less cost for agencies that have a geographically dispersed footprint. The Core + Edge configuration has yielded much tighter voice communication integration between locations and also a highly fault tolerant network. Avaya collaboration applications, such as the Call Center Elite application, allow agencies to have call center agents geographically dispersed across the county, yet they appear as a single work group from a citizen facing standpoint.

The system architecture is also integrated with a new Call Management System (CMS) solution from Avaya. This solution's capability greatly improves the collection of necessary statistics used by Contact Center Managers to evaluate the county's responsiveness to citizens and constituents.

5.4.5 Public Service and Public Safety Radio Networks

The county operates two voice radio 800 MHz trunked radio systems, one dedicated for public safety emergency response operations with over 6,000 units, and the other that supports more than 3,000 radios for Fairfax County Public Schools Transportation (school buses), and county agencies including the Department of Public works and Environmental Services, Park authority, FASTRAN, the CONNECTOR bus system, and other non-public safety county agencies. The county's planning effort for a Public Service Radio System Upgrade will begin in FY 2013 with implementation commencing in FY 2016.

The past two years county staff in conjunction with Motorola Systems has been implementing the Public Safety Radio system upgrade project which is scheduled for completion in October 2012. This new system incorporates a digital IP-based technology permitting

improved data access and system management, better integration with the new Computer Aided Dispatch system (Intergraph), improved regional interoperability, and the inclusion of a new tower in Bailey's Crossroads for improved system coverage. The two radio system infrastructures, Public Safety and Public Service, are architected to allow interconnection, as well as back-up capability for each other.

The FCC mandated 800 MHz re-banding effort is targeted for July 2013. County staff not only manages the county's –systems transition, but also serve is the Regional Coordinator for the entire National Capitol Region's re-banding effort to assure that regional interoperability is maintained.

5.5 Internet Architecture

Fairfax County's Internet architecture supports the County's e-Government program which utilizes emerging WEB technologies to make county services and information readily accessible and available to the public, with interactive services to conduct business (e.g., pay taxes,

apply for permits, etc.), and searchable access to data (real estate assessments, Human Services resources, etc.). The e-Government architecture defines the standards, technologies and guidelines for public access, and requirements for conducting on-line business with county

agencies, state agencies and outside entities. To meet the demand of changing times and recognizing mobile technology is key to communications, the county's e-Government program has taken the initiative (m-Government) to provide mobile access that enables greater interaction and service delivery such as mobile device-compatible web access and applications.

The county's internet architecture is comprised of the following:

- **High Speed Connection to the Internet** – The county's fractional DS-3 connections to the Internet provide internet access for county staff as well as outside access to the county's Web server(s) by residents, business, and others via the Internet.
- **Public Access Web Server** – The county's Public Access Web Server provides Internet users with a vast amount of information made available by various agencies. The Web server can be viewed as an "on-line service counter" where residents and others may obtain information related to services, licenses, taxes, recreation, court filings, etc. The Web server also acts as the distribution or collection point for information obtained from or provided to enterprise databases via an "Application Server".
- **Intranet Web Farm** – The county InfoWeb Intranet Web farm provides a portal access to county information and applications for agency and employee use.
- **Mobile Web Farm** – provide mobile phone users with information made available by county agencies via Web Content Management by county agencies via Web Content Management systems in a mobile device-friendly format, thus allowing citizens to obtain information and conduct e-service transaction via mobile devices. The mobile web farm also enables county developers to continuously develop more web-based mobile applications to transition the county from 'e'-government to 'm'-government.
- **iPhone Application Infrastructure** – iPhone Application for release for release into Apple's App Stores allows iPhone users to access county's web contents and interact with various county e-services. SDK environment, iPhone application template, standards, and App Store distribution channel have been developed to further enable county to provide m-government services.
- **Interfaces** – between the county application servers and the enterprise databases provide the link that allows access to data residing in a wide array of sources. The interfaces make it possible to access data from virtually all of the county databases: Oracle, SQL, MS Access, DB2 and VSAM. The interfaces are comprised of "Application Program Interfaces" (APIs), Open Database Connectivity (ODBC), SOA, and other standards that enable the access layer of the web architecture.



5.6 Security Architecture

The Information Security Office defines and enforces the security standards and policies necessary to protect the county's information assets and technology infrastructure. IT Security continues to be a fundamental component of the county's enterprise architecture and e-Government strategy. The security architecture fuses best practice security principles with a hardware and software infrastructure, supported by policies, plans, and procedures. This layered architecture is designed to provide an appropriate level of protection for all county information processing resources, regardless of platform, and includes incorporation of industry best practices to yield an overall reduction in risk.

The objectives of the information security program are to ensure confidentiality of information, integrity of data, systems and operations, technical compliance with legal mandates such as HIPAA and PCI, privacy and availability of information processing resources. The information security program utilizes a multi-faceted approach to meet these objectives, an approach that includes threat reduction techniques, technology and management solutions, and the vigorous implementation of awareness activities. The basic elements of identification, authentication, authorization, access control, and monitoring of information processing activities are employed throughout the enterprise. The secure network architecture is best described as a defense-in-depth approach to network security design, to include a method of secure network segmentation. In this architecture, modular infrastructure building blocks are deployed to better shield important resources within the network.

The "SAFE" network architecture was developed and deployed to divide the network perimeter into the following five business groups: E-Commerce, Internet Access, Partners, Emergency Operations, and Public Access. Each group is protected by its own physical firewall, with firewall policies tailored to each specific business area. This strategy has optimized firewall performance and limited risk exposure to each business group.

- The E-Commerce business group supports all public facing web services providing access to county resources for both citizen and business.
- The Internet business group is used to control county employee access to the internet and allow for content and virus scanning.
- The Partners business group allows for connections to external "Trusted Partners" to include Fairfax County

Public Schools, Fairfax County Water Authority, Commonwealth of Virginia (State Police, State Health, Department of Social Services, Supreme Court of Virginia, Department of Juvenile Justice, and State Board of Elections) as well as public safety connections for several adjoining jurisdictions.

- The Emergency Operations group was established to secure the Emergency Operations Center providing IT resources to the Department of Emergency Operations.
- The Public Access network was built for the Libraries and Community and Recreation Services.

Remote access via VPN and Citrix services provides access to the county's Enterprise Network resources for telecommuters, vendors, remote access users or business travelers, as well as several small Fairfax County offices. Security for remote access is managed through a Remote Access Server using security tokens and PIN numbers. Additionally, IT Security plans to acquire and implement a mobile security solution which can begin to address the challenges of data loss prevention and security on mobile devices, such as tablets and smartphones, which may access county data from remote networks.

Firewall technology is used as the main perimeter defense with all access from the Internet routed through the county's system of firewalls. In addition, the county configures broad network traffic filtering and selective routing at firewalls provisioned nearest to the county's Internet peering points, reserving more granular filtering and routing for network traffic transiting to the internal network connection. Classic authentication for each internal user is based upon a unique UserID (also called a sign-or log-on) combined with a unique, strong password. To improve the secure access and authentication to web-based applications and backend servers, the county has implemented an identity management platform that positions DIT to leverage the security architecture framework well into the future. CA e-Trust, through its SiteMider module, provides a software platform of shared services that includes reduced sign-on, authentication management (to validate who you are), and entitlement management (to authorize what you are allowed to do on the site) for web-based applications. eTrust also provides a secure reverse proxy solution that passes requests to enterprise backend content servers, and returns resources to the requesting client, thus allowing for a practical solution for the protection of internal assets. With Identity Management

in place, the county can manage user profiles for both internal staff and public access, making personalized e-Government a reality. Expansion of eTrust will continue in order to provide a secure access and an end-user authentication platform for external users. As part of the implementation of FOCUS, the SAP IDM solution provides for user provisioning between the county and schools enterprise networks.

Intrusion Detection System (IDS) detect intrusions within the network, and Intrusion Prevention Systems (IPS) primary function is prevention rather than detection. IPS devices can proactively prevent intrusions by detecting signs of an intrusion and/or detecting an actual intrusion attempt. IPS provides capacity to perform real-time analysis of intrusion attempts to determine if sensitive data, systems or network devices are being attacked or if a breach of confidentiality, integrity, or availability has occurred. The primary objective of Intrusion Prevention is to reduce damage and isolate/ contain malicious traffic. With the large quantities of log and alarm data generated by firewalls and sensors, a specialized application to support the role of correlation and alerting has also been implemented. The IPS solution conducts a comprehensive threat assessment and allows for quick identification of credible threats to the organization in order to facilitate expedited response and containment of intrusions and malicious activity.

As the key aspect of the IT Security strategy, the county employs a private/public network model. Sensitive and critical assets are located on the private portion(s) of the network while information and services available for public use are located on the public segment(s). CITRIX,

VPN, Web Access and dial-up technologies are available for remote users. Each of these services requires a personal security token and LDAP-based authentication for access, otherwise known as two-factor authentication. Remote access is approved at the same level as if the user were physically at their work site. Identification and authentication, access control, and auditing functions are performed on the specific platforms using the capabilities inherent in the appropriate operating system. Mandates such as HIPAA and the Payment Card Industry (PCI) standard have increased system monitoring and policy enforcement requirements. IT security awareness activities have been implemented to effect a culture change for all employees. Through security conscious employees, realization of the return on investment in security technologies can be leveraged further as the overall risk to data and systems is reduced.

The Fairfax County Government is dedicated to the protection of its IT assets and the data & information in its charge. The county is also dedicated to the task of ensuring that no unauthorized access or use of such data and information occurs. As evidence of its long standing, best practices approach and implementation of IT Security, the Fairfax County Government received Cybertrust's Enterprise Security Certification in May 2010.

The Security Management Program (SMP) is a comprehensive security assessment and certification program that validates an organization's security posture. This certification attests that Fairfax County Government has made security a priority, and employs renowned security processes and technologies in the establishment and maintenance of a proactive and





comprehensive information security program. The certification also acknowledges that the county's information security controls, policies and procedures have been examined, measured and validated against a stringent set of generally accepted enterprise security

5.7 Technical Architecture

The Department of Information Technology establishes, updates, and retires technical standards throughout the year to ensure alignment, consistency, and modernization in the selection and design of business solutions across the county.

A platform is established as a standard through a governance process. This approach enables DIT to define and develop a portfolio of technology solutions that can be effectively managed and supported given available resources. Typically, projects in the concept stage come before DIT's **Architectural Review Board (ARB)** to discuss the technical approach and business objectives. Where the concept relies on new products or non-standard configurations, the details are assessed to establish general conformity to enterprise objectives. The ARB may steer the solution back to conformance, or it may authorize the use of a new product or configuration by granting a waiver. The ARB may alternatively recommend that the new product replace an existing standard, or that it be added to the list of supported standards. When DIT's executive management approves a recommendation, the standards are updated accordingly. Once adopted, the new product and its former standard, if any, are further classified as emerging (new), current (established), twilight (becoming obsolete), or sunset (referring from support as of a known date).

When a standard is established, it indicates that the designated technology will be supported by DIT as applicable, and that the selection is in alignment with broader IT goals, objectives, and strategic direction. In some cases, a standard may be adopted in advance of procurement or deployment, to provide strategic direction for emerging business needs. Adoption of a

requirements. The SMP utilizes proven International Organization for Standardization / International ElectroTechnical Commission 27002 security controls and helps customers such as Fairfax County Government prioritize and identify security risks in an ongoing manner, and then proactively manage threats before they have an impact. Fairfax County is the only local government within the National Capitol Region that holds this certification.

standard is not intended to convey endorsement for, or recommendation against, any specific product.

Declaration of a standard product(s) indicates DIT's strongest recommendation for selection of the available product(s) over any alternatives that may be similar or comparable. Generally, any solutions that will rely on the systems enterprise infrastructure, connect to the network, or depend upon DIT support must be fully conforming. Agencies using or selecting non-standard solutions may apply to the Architectural Review Board for a waiver on the basis of business needs and justification.

Standards are essential to sound cost controls in software licensing and maintenance, hardware, services, training, and integration. Having fewer platforms in use enables allocated resources to better support the information systems under management. Agencies are encouraged to invite DIT members to participate in selection and technical advisory committees for the Request for Proposal (RFP) process. In some cases, DIT and its ARB should be consulted in advance of an RFP, to help explain technical alternatives and develop the proposal language to support conformance with existing and emerging standards.

The standards shown here do not represent a comprehensive view of all the products in use across the County. The list is intended to convey the primary standards for the major solutions to be supported by DIT and/or delivered with DIT resources.

Revised June 2013

**FAIRFAX COUNTY INFORMATION TECHNOLOGY ARCHITECTURE
PLATFORM ARCHITECTURE: END USER SOFTWARE**

Component	Environment
Operating System	Windows 7 / 8
Word Processor	Microsoft Word 2010 / 13
Spreadsheets	Microsoft Excel 2010 / 13
Presentations	Microsoft PowerPoint 2010 / 13
Database	Microsoft Access 2010 / 13
E-Mail Client	Microsoft Outlook 2010 Outlook Web Access (latest release)
Project Management	Microsoft Project Professional (latest release)
Graphics	Microsoft Visio Professional (latest release)
Web Browser	Microsoft Internet Explorer – IE8
Antivirus	Symantec AntiVirus (latest version) for Workstations and Servers
Patch Management	Microsoft System Center Configuration Manager (SCCM) 2012 Windows Server Update Services (WSUS)
Mainframe Terminal Emulation	Blue Zone
Thin Client Access	Citrix Xenapp 6.5 / Desktop 6.0
Other	Must be approved for Business Unit standard image/requirements

**PLATFORM ARCHITECTURE:
END USER HARDWARE**

Component	Desktops	Laptops	Tablets
Power	Single	Single	Single
CPU	Intel Quad Core i7 -3770, 3.4GHz Optiplex 9010	Intel Core i5-3340, 2.7 GHz E6430	i5-3337U (3M Cache, up to 1.80 GHz
Disk Configuration	250 GB, SATA Drive	250 GB, SATA Drive	128 GB SSD
Disk Configuration	500 GB, SATA drive	320 GB, 5400 RPM Hard Drive	128 GB SSD
Media Drive	16X DVD R/W combo drive	8X DVD CD-R/W combo drive	
Memory	8 GB, Non-ECC DDR3, 2 DIMMS	4 GB, SDRAM (1 DIMMS)	4 GB
Monitor	22" Economic, Flat Panel, DVI/VGA	14" Wide Screen WXGA+ LCD Panel	11.6" Full HD (1920 x 1080) IPS (400 NITS)
Video Card	Integrated Graphics DP/DP/ VGA w/DP-to-DVI Adapter	Intel® HD Graphics 4000	Intel HD Graphics 4000
Interface Card(s)	Ethernet 10/100/ 1000 Base-T	Built-in 10/100/1000 GB Ethernet card	None – 3rd Party USB to Ethernet
Wireless	N/A	Intel Centrino Advanced N 6205 802.11 a/b/g/n	Intel Centrino Advanced N 6235 802.11 a/b/g/n
Operating System	Windows 7 / Window 8	Windows 7 / Windows 8	Windows 8
File System	NTFS	NTFS	NTFS
Maintenance	5 Year on-site, next business day	5 Year on-site, next business day	3 Years on-site, next business day
Additional Hardware Requirements	Sound bar not included	Port replicator, external mouse, keyboard and monitor if used as desktop, Security Lock	Keyboard, and Port replicator

**PLATFORM ARCHITECTURE STANDARDS:
HAND HELD MOBILE DEVICES**

Component	Environment
Platform/Devices	RIMM/Blackberry Syclo Blackberry Enterprise Server iOS (iPhone, and iPads) Androids phones and tablets
Software Compatibility	Outlook Exchange (Downloadable) Date Book, Address Book, To do List, Memo Pad, Calculator
Connectivity	TCP/IP Internet or USB enabled

PLATFORM ARCHITECTURE: Server Standards

General Server Standards: Servers needs are determined based on many factors, including utilization of existing infrastructure, requirements of planned projects, and the availability of specific funding for new equipment. Some platforms will share components and others will not, depending upon the unique circumstances for each project and product. Sharing and re-use are promoted when feasible. The county's goal is to provide a homogeneous environment to streamline support and maximize resources, using virtual environment and consolidated server farms supporting many applications.

**PLATFORM ARCHITECTURE:
GENERAL SERVERS**

Component	Environment
Operating System	Microsoft Windows Server 2012 Enterprise Edition Solaris (latest release) z/OS 1.4
Thin Client Access	Citrix Xenapp 6.5
Hardware	Intel (Windows) SPARC (UNIX) HP UX IBM Z-Series (Mainframe)
Backup	Symantec Net Back Up z/OS DFSMS Net App snap shots
Storage	IBM XIV (SAN) NetApps (NAS) EMC Data Domain
E-Mail	Microsoft Exchange Server 2010/2013 Enterprise Edition L-Soft LISTSERV
Web/Application Servers	Preferred: Microsoft Internet Information Server – IIS7 Apache Web server (if required by COTS package) Tomcat (if required by COTS package) JBOSS BEA Systems WebLogic Microsoft BizTalk Web Methods Oracle Application Server 11g
Configuration/Change Management	VSM (Infra Enterprise) – ITIL Service Management

**PLATFORM ARCHITECTURE: FILE/PRINT/WEB SERVERS:
SERVERS WILL BE VIRTUAL WHENEVER POSSIBLE.**

Component	File/Print/Applications/Web (INTEL)	Database Server (INTEL)	Web Server/Application (UNIX)
Type	INTEL	INTEL	UNIX
Power	Redundant, UPS required if not EOC-resident	Redundant, UPS required if not EOC-resident	Redundant, UPS required if not EOC-resident
Fault Tolerance / Disk Configuration	Operating System Drives – Raid 1 (Mirrored) Database / Application Drives – Raid 5 utilizing SAN if EOC resident	Operating System Drives – Raid 1 (Mirrored) Database / Application Drives – Raid 5 utilizing SAN if EOC resident	Operating System Drives – Raid 1 (Mirrored) Database / Application Drives – Raid 5 utilizing SAN if EOC resident
CPU	Dual 3.0 MHz	Dual 3.0 MHz	Dual 1.5 GHz
Network Interface Cards	Dual Ethernet 1000 Base-T	Dual Ethernet 1000 Base-T	Dual Ethernet 1000 Base-T
Operating System	Windows 2008 R2 Server	Windows Server 2008 R2	Solaris (latest release)
Monitor	17" SVGA Color, if non-EOC site Not required if EOC resident	17" SVGA Color, if non-EOC site Not required if EOC resident	Rack mountable Flat LCD monitor Required if EOC resident
RAM	16 GB Minimum Cache 256 MB	16 GB Minimum Cache – Database/ Application specific	16 GB Minimum Cache – Database/Application specific
File System	NTFS	NTFS	Solaris
Third Party Software Requirements	Symantec Antivirus, Enterprise Edition MS SCCM Client	Symantec Antivirus, Enterprise Edition eTrust SiteMinder Agent MS SCCM Client	Symantec Endpoint Protection Enterprise Edition eTrust SiteMinder Agent
Web Server Software	N/A	Internet Information Server IIS7 Tomcat (if required by COTS package) BEA Systems WebLogic	Apache (if required by COTS package) Tomcat (if required by COTS package)
Platform	Dell	Dell	Sun
Maintenance	5 Year, 24/7, 4 hour on-site, parts & labor included	5 Year, 24/7, 4 hour on-site, parts & labor included	5 Year, 24/7, 4 hour on-site, parts & labor included
Additional Hardware Requirements	Raid Controller Rack mountable rails if EOC resident Minimum 3 Open Slots to facilitate system expansion HBAs (if connected to SAN)	Raid Controller Rack mountable rails if EOC resident Minimum 3 Open Slots to facilitate system expansion HBAs (if connected to SAN)	Raid Controller Rack mountable rails if EOC resident Minimum 2 Open Slots to facilitate system expansion Dual HBAs (if connected to SAN); DVD-ROM & Tape Drive (DDS-4)
Pre-Install Options	None	None	None
Storage And Backup	Symantec NetBackup (i.e. snapshot)	Symantec NetBackup (i.e. snapshot)	Symantec NetBackup (i.e. snapshot)

**PLATFORM ARCHITECTURE:
DATABASE/APPLICATION SERVERS**

Component	Mainframe Sun-setting	UNIX	INTEL	WEB	GIS
Database Software	N/A	Oracle 11g	SQL Server (latest release) Oracle 11g	N/A	Oracle 11g Oracle Spatial DB
Application Development Frameworks	N/A	Java 1.6 or newer	.NET Framework (latest release) Java 1.6 or newer	.NET Framework (latest release) Java 1.6 or newer	.NET Framework (latest release) ESR Pictometry
Virtualization	LPARS	Zones/Containers HPVM	VMWare	VMWare	Zones/Containers
Software And Development Tools (Report Writing Products Are Listed On Page 8.)	COBOL CICS TSO JCL	N/A	Microsoft Visual Studio – Latest Release Eclipse	Microsoft Visual Studio – Latest Release Eclipse	ArcGIS 9.3 & Extensions ERDAS 9.3 Arc Internet Map Server 9.3 /ArcGIS Server 9.3 ArcSDE 9.3 ArcPad 8 OnPoint 6.2 Microsoft Visual Studio – Latest Release
Version And Release Control	SCLM	Serena Version Manager	Serena Version Manager	Serena Version Manager	Serena Version Manager
LDAP / Directory / Authentication	RACF	Native operating system (Solaris, Linux, AIX)	Active Directory e-Trust SiteMinder	Active Directory e-Trust SiteMinder	Native Operating system
Data And Process Modeling	MS Visio Professional – Latest Release	MS Visio Professional– Latest Release	MS Visio Professional – Latest Release	MS Visio Professional – Latest Release	MS Visio Professional – Latest Release
Middleware (EAI)	webMethods Jacada	webMethods	webMethods MS BizTalk	webMethods Jacada MS BizTalk	N/A
Workstation Requirements	TCP/IP Connectivity	Oracle Client Suite ODBC Drivers	Oracle Client Suite ODBC Drivers SQL Management Studio	MS Internet Explorer – IE8 in IE7 mode	Terminal Server Client Citrix Metaframe Client Active X Plug-in Active Directory Tools

**PLATFORM ARCHITECTURE:
ENTERPRISE SOLUTION PLATFORMS**

Platform	Current Standards
Report Writing: Departmental Reporting Needs	Business Objects Crystal Reports Microsoft SQL Reporting
Statistical Analysis	SAS
Enterprise Reporting Business Intelligence	SAP/BOBJ
Document Scanning/Imaging	Documentum Enterprise Content Management / Captiva
Web Content Management	Documentum Web Content Management
Web Search Engine	Google Appliance
Survey Instrument Software	SNAP 8.0 ProNet Edition (w/Scanning module)
Correspondence Tracking	Intranet Quorum
CRM	Siebel / Microsoft Dynamics
IT Services Management	VSM (Infra Enterprise)
GIS	ArcGIS 9.3 & Extensions ERDAS 9.3 Arc Internet Map Server 9.3 / ArcGIS Server 9.3 ArcSDE 9.3 ArcPad 8 OnPoint 6.2 Electronic Field Study 2.7
ERP	SAP core; ESS, MSS portal
Voice Communications	Avaya S8700s and G700s Servers