GeorgiaJDX

Strategic Data Sharing for Justice

GEORGIA-INFORMATION SHARING ENVIRONMENT (G-ISE)

SOLUTION ARCHITECTURE

Version 4.0

November 2010

Table of Contents

1 Overview

Georgia's criminal justice agencies have initiated a statewide effort to integrate their operations through a transformed criminal justice enterprise. This project, Georgia Justice Data Exchange (GeorgiaJDX), strives to define an architecture that supports the following vision:

- Enables users with the appropriate levels of access to request criminal information at any time from any place and to receive complete and accurate information in a timely manner
- Creates opportunities for cost savings by promoting efficient administration of individual criminal justice functions
- Creates a distributed, protected and trusted environment for data sharing
- Provides mechanisms to permit criminal justice agencies at the Circuit and County levels to share data based on common standards and practices
- Supplies capabilities to discover and link justice information on a statewide basis, including detecting relationships among people, places, things, and events
- Leverages applications and networks currently utilized by participating agencies
- Enhances strategic decision making capabilities through improved access to relevant data
- Ensures the availability of current, valid statistical information to support monitoring and assessment of the Georgia criminal justice system
- Supports proactive caseload management and heightened accountability relative to state and federal guidelines and procedures
- Improves public safety in a cost effective manner

Key to the long-term success of the GeorgiaJDX project is development and statewide adoption of comprehensive solution architecture. The envisioned GeorgiaJDX architecture will provide a framework that leverages existing systems, processes, policies, and information to the maximum practical extent. It will reflect ongoing national standards initiatives, including the Justice Reference Architecture (JRA) and the Global Federated Identity and Privilege Management (GFIPM) being developed by the Global Infrastructure/Standards Working Group (GISWG) and the Global Security and Privacy Group through the auspices of the US Department of Justice, and the National Information Exchange Model (NIEM) being addressed through the leadership of the US

Department of Justice (DOJ) and the US Department of Homeland Security (DHS). An overview of the Justice Reference Architecture as defined by the DOJ Office of Justice Programs (OJP) is provided in Section 1.1 below. Section 1.2 defines the Service Oriented Architecture (SOA) that is central to the Justice Reference Architecture and the concept of services.

Since components of this large and complex effort will be deployed incrementally, it is critical that all components are designed, developed and/or acquired and implemented in a manner supporting interoperability and based on national standards. ***This Solution Architecture document provides a vision and a roadmap to guide these developments and implementations***. Solution Architectures are structured, technical documents scoped to describe the particular functions or processes to be implemented, identify operational outcomes, and define specific information technology assets, applications and components for procurement, development and implementation. This GeorgiaJDX Solution Architecture will be used to guide the implementation of the information sharing capability across the State of Georgia. The Solution Architecture sets the direction and provides incremental steps toward the targeted capability of a Georgia-Integrated Sharing Environment (G-ISE). It addresses three objectives:

1. Provides a comprehensive, high-level description of the GeorgiaJDX architecture
2. Establishes the architectural framework for implementing the GeorgiaJDX capabilities
3. Identifies key architectural decisions that have been made or must be made

Solution Architectures do not specifically identify vendors or specific vendor items as these are generally identified in subsequent specification documents and/or procurement orders. Additionally, Solution Architectures do not focus on enabling technologies such as case and records management systems criminal justice agencies utilize to manage and administer their workloads. It is assumed these technologies either exist or will be procured. Rather, the Solution Architecture defines the standards, functions and processes that must supported by these enabling technologies so they can effectively participate in the information sharing system.

This document is intended for senior leadership, program managers, chief architects, systems designers, network managers, and information technology implementers associated with the GeorgiaJDX project. The purpose of this document is to provide guidance during the procurement and implementation of end-point solutions to ensure each fits into the overall enterprise architectural framework.

1.1 Justice Reference Architecture Overview

The following excerpt from the DOJ Office of Justice Programs website is an overview of the Justice Reference Architecture. This excerpt provides high-level definitions of the JRA components that are described in this document in the context of the GeorgiaJDX Solution Architecture.

The Global Justice Reference Architecture (JRA) is an information exchange solution designed to cut 80 percent of implementation time and costs for state and local justice agencies through reuse of established promising practices in IT architecture and design. Efforts to develop a reusable information sharing solution specific to the justice domain began in the Global Infrastructure/Standards Working Group (GISWG), specifically the Services Task Team (STT), with leadership from Thomas Clarke and James Douglas. Today, the STT serves two functions: 1) the creation of new Reference Service Specifications to provide the opportunity for reuse in the field, and 2) review of JRA implementations that have the potential for reuse by other agencies. Additionally, the STT recently identified the most critical information exchange priorities for the national justice community through the input of representatives across the justice domain, publishing the results in the Priorities Definition Workshop Summary Report.

Global JRA Services in Further Detail

The Global Infrastructure/Standards Working Group (GISWG) has authored the working draft document titled Global Justice Reference Architecture Services to describe in detail Global JRA services, Service Specification Packages (SSPs), and the Services Task Team (STT). This information is meant to help current and potential users better understand JRA and its components.

JRA Components

The JRA addresses various areas in the implementation of information exchange. Together, these areas form critical components of a comprehensive, replicable, and

scalable solution to information sharing that balances varied technologies with dynamic policy considerations:

- ***Reference Architecture Planning*** *- The Global JRA includes recommendations for technical implementation that leverage Service Oriented Architecture concepts, customized for the justice domain. JRA addresses the full range of information sharing use cases by providing a flexible blueprint for implementing interoperable data sharing services across both technologically advanced organizations and those with limited technology resources.*
- ***Service Specification Packages*** *- JRA solutions to information exchange are made up of a combination of the connection method (often Web Services), the exchange language (use of NIEM is encouraged), and the security specifications (encryption at the transport layer, data layer, etc.). These specifications are packaged into a JRA solution that can be customized to meet an individual organization's needs. A repository of Reference Service Specification Packages (SSPs) for information exchange in the justice community is being established.*
- ***Technical Implementation Guidance*** *- Integrating a Reference Service Specifications Package (SSP) into existing IT infrastructure, despite the level of customization available in a Reference SSP, can involve a learning curve for those new to the implementation of JRA. Technical guidance regarding the JRA specification itself, as well as various guides on the interaction of different services and other aspects of information exchange [is available].*
- ***Policy Guidance*** *- In coordination with the technical implementation of a JRA Reference Service Specification Package, policy-level documents guide interaction between the agencies exchanging information. Examples include Service Level Agreements (SLA), access and identity management specifications, Memoranda of Understanding (MOUs), and many others. While these documents are never specific to JRA implementations, some specific resources [available on the DOJ OJP website] may be helpful in [defining] policy agreements.*[1]

[1] http://it.ojp.gov/default.aspx?area=nationalInitiatives&page=1015

1.2 Service Oriented Architecture (SOA) and Services Overview

Service Oriented Architecture is a methodology for integrating systems while maintaining as much of their autonomy and independence as possible. SOA allows systems to share information in a manner that allows them to change independently, thus enabling the JRA focus of interoperability at the system interface level rather that at the systems themselves.

An SOA separates information sharing partner capabilities into distinct units known as services. A service is the means by which one information sharing partner system gains access to the capabilities of another information sharing partner system. Services are accessible over a network so users can combine and reuse them to provide and receive real-time information. Services communicate with each other by passing data from one service to another or by coordinating an activity between two or more services.

Section 3 discusses business services, such as exchanges and queries, and the enabling services that provide management and administrative support for business services.

1.3 Document Organization

Below is a brief description of each of the following sections of this GeorgiaJDX Solution Architecture document. We acknowledge the technical specificity of Section 3, which describes functional, logical and technical perspectives of the GeorgiaJDX Solution Architecture. While we strive to define terms and concepts for all readers, this section must be described in technical detail to provide a thorough roadmap to effectively guide the GeorgiaJDX project.

Section 2: Current Environment. This section discusses the current state of information sharing across the State of Georgia. It outlines the roles and responsibilities of the stakeholders and the business, technology, application, data, network, information sharing and security architectures that currently exist at the city, county, circuit and State levels.

Section 3: GeorgiaJDX Solution Architecture. This section discusses the proposed solution architecture for the GeorgiaJDX project from functional, logical and technical perspectives. It also describes how the proposed architecture conforms to the Justice Reference Architecture (JRA) developed by the Global Infrastructure/Standards Working Group (GISWG) of the Global Advisory Committee (GAC) and to National Information Exchange Model (NIEM) data standards.

Section 4: Action Plan. This section outlines an action plan for the GeorgiaJDX project. It identifies the short-, medium- and long-term initiatives to be developed and implemented.

Section 5: Governance Model. This section discusses the role of governance in the GeorgiaJDX project and proposes a governance model to manage the information products to be produced through GeorgiaJDX project and the various standards those products will incorporate.

Section 6: Conclusion. This section concludes this GeorgiaJDX Solution Architecture document.

2 Current Environment

This section documents the current information sharing environment across the criminal justice community at the county, circuit, and the State levels in the State of Georgia. Highlights are provided for the statewide criminal justice enterprise and for the existing business, technical, application and data, information sharing and security architectures. The findings in this section highlight the importance of addressing information sharing from an enterprise perspective and illustrate various challenges that can be overcome by adoption and application of the proposed GeorgiaJDX Solution Architecture, including:

- Duplicate entry of data into multiple systems, a time-consuming and inefficient practice that often leads to inaccuracy due to input errors
- Delayed access to accurate information
- Varied levels of automation across the criminal justice community
- Inconsistency of process across agencies

- Inability to leverage existing technology to reap process efficiencies due to lack of knowledge and awareness
- Minimal connectivity across agencies at the local level
- Inconsistent levels of Information Technology (IT) support across Counties and Circuits
- Myriad disparate vendor commercial-off-the-shelf (COTS) and custom developed case management and records management systems, many of which are not based on national standards
- Siloed systems that support functional requirements of the owning agency but are not architected to support information sharing
- Inconsistent and inadequate security measures applied to current information sharing processes
- Low acceptance rates of dispositions resulting in accurate data in Computerized Criminal History records
- Inaccurate caseload statistics

All these issues result in process redundancies and workarounds that impose additional costs to Georgia's criminal justice agencies. These challenges also negatively impact, and result in inefficient delivery to, clients of the agencies – the citizens of the State of Georgia. The proposed enterprise approach presented in subsequent sections of this GeorgiaJDX Solution Architecture document will enable diverse systems, processes and initiatives to focus on the common goal of creating an information sharing framework that enables all participants to share accurate information in a timely manner. Benefits of this approach, which emerge as common themes going forward, include:

- Enables the enterprise to adopt and utilize current data and technology standards
- Encourages reusability, resulting in cost efficiencies across the State of Georgia
- Isolates individual agencies from the impacts of modifications and functional issues to other agency systems
- Empowers the overall justice process to become more efficient, resulting in cost savings to individual agencies, improved service delivery and enhanced public safety

2.1 Georgia Criminal Justice Environment - Overview

The State of Georgia comprises 159 counties, 49 circuits and ten districts. Numerous agencies in each county support justice functions, and processes and procedures are not standardized across jurisdictions. The Georgia constitution empowers its citizens at the local level, with much of that power vested in elected judges, prosecutors, clerks, sheriffs, and local governing bodies. These local elected officials have achieved significant success towards the goal of creating an integrated justice information sharing system. However, significant additional work is required to optimize information sharing statewide.

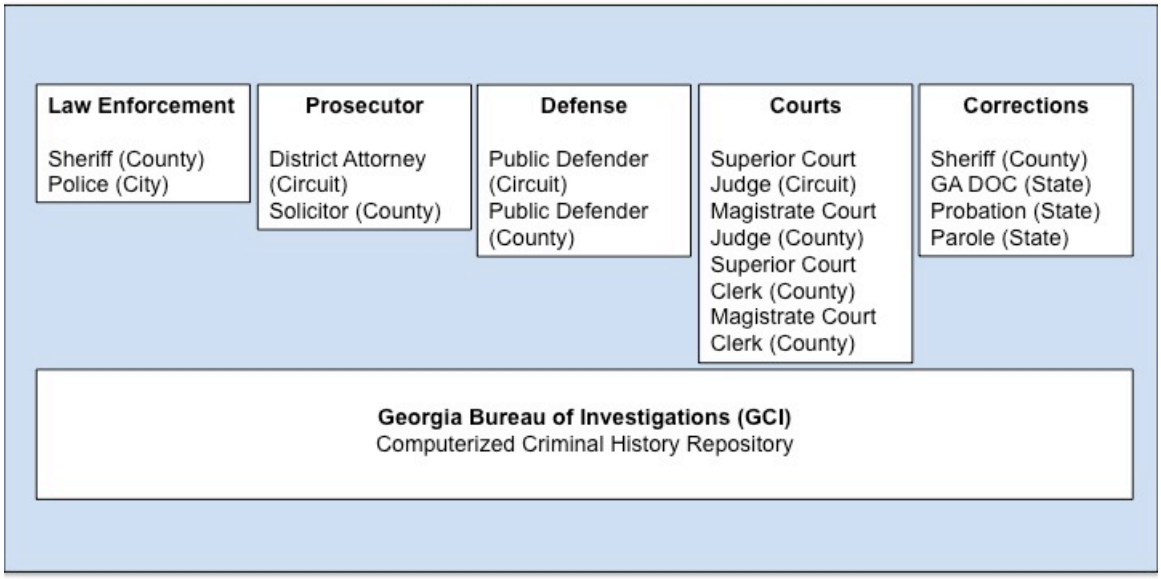
The US Department of Justice Bureau of Justice Statistics developed an Offender Lifecycle[2] that defines the justice functions and activities occurring across the Offender Lifecycle. These functions are:

- Law Enforcement
- Prosecution
- Courts
- Corrections

Each function interacts with the state criminal history repository to extract and update information on the offender as the offender progresses through the justice functions. The current Georgia Criminal Justice Enterprise follows this overall model. However, multiple organizations at the State, circuit, county and city level perform the same functions. Figure 1 depicts the various organizations in Georgia performing the criminal justice functions identified in the Offender Lifecycle and identifies the level at which each organization functions.

[2] Adapted from The Challenge of Crime in a Free Society, President's Commission on Law Enforcement and Administration of Justice, 1967

Figure 1: Organizations Conducting Criminal Justice Activities in Georgia



2.2 Business Architecture

Outlined below is the general information flow between the various criminal justice agencies in Georgia for the Criminal Warrants process that initiates the Offender Lifecycle referenced in Section 2.1. The type of scenario dictates the organizations and individuals that may be involved in the process. For example, the process flow below assumes Law Enforcement is the requestor of the Warrant and further assumes the warrant request is not Civil in nature.

While variations exist in how some counties and circuits conduct their business processes, the general steps in the warrant processing information flow are as follows:

1. Law Enforcement agency records an incident
2. Law Enforcement agency applies to Magistrate for warrant
3. Magistrate issues warrant and sends it to Sheriff for serving (or to agency applying for warrant – varies by county)
4. Upon arrest, Sheriff books offender into Jail
5. Sheriff takes fingerprints and submits prints to Georgia Crime Information Center (GCIC) if finger-printable offense
6. Sheriff assigns Offense Tracking Number (OTN) and Charge Tracking Number (CTN); GCIC tracks offender by OTN and CTN

7. Sheriff sends warrant served information to clerk of appropriate court having jurisdiction over the offense
8. Clerk of Court delivers warrant served information and related documentation to prosecuting attorney
9. District Attorney creates Indictment or Accusation and sends to Clerk of Superior Court
10. Clerk of Superior Court initiates case
11. Case is processed in Courts
12. Upon case resolution, Disposition information is sent to various local criminal justice system stakeholders and to GCIC
13. Clerk of Superior Court prepares Sentencing packet and sends to State Department of Correction if defendant is convicted of a felony and sentenced to confinement
14. State Department of Correction receives Sentencing Packet
15. Process for transferring offender to State custody commences

2.3 Technical Architecture

The current technical architecture and sophistication of automation across Georgia counties varies considerably. For example, while some stakeholders such as the Clerk of Courts, District Attorneys, Solicitor and Judges have robust case management systems, many Sheriffs' Offices rely on older legacy systems.

From an infrastructure perspective, the Clerk of Courts and the District Attorneys share a network that enables them to connect with their peers. However, minimal connectivity exists among criminal justice agencies at any level.

Information Technology support is similarly inconsistent, ranging from skilled to no internal IT staffing. Many vendor-provided applications are supported through annual maintenance contracts.

2.4 Application Architecture

Numerous applications, both vendor-provided COTS packages and custom-developed solutions, support Georgia's criminal justice agencies. Each type of agency utilizes case or records management systems, some provided by recognized industry leaders and

others custom built internally or by contractors. These disparate applications typically have unique databases and business logic and may not communicate easily with others without custom point-to-point interfaces. Adoption and utilization of standards will mitigate the need for custom interfaces. Table 1 depicts the most common vendor applications utilized by each type of criminal justice organization.

Table 1: Agency Applications

Type of Agency	Common Vendor Applications
Police Departments	Eagle, Intergraph, Police Central
Clerk of Courts	ICON, Iron Data, Sustain, custom development
Sheriffs	Comnetix, Digital Solution Inc, Eagle, Police Central, Spillman
Magistrates	ICON, Sustain, custom development
District Attorneys	Prosecutor Dialog, Tracker (Statewide)
Solicitors	ICON, Tracker, custom development

2.5 Data Architecture

Each of the applications identified in Table 1 was selected or developed to support specific functional needs of the adopting agency, and its data architecture was designed accordingly. For example, the Sheriffs' applications assign an Offender Tracking Number as the mechanism for the tracking an offender. The OTN is used to track the offender event in both the Sheriffs' systems and GCIC. Court applications are driven by the Case Numbers assigned to each case. In addition to differing master records (i.e., OTN, Case Number, etc.) the data elements and the set of values within each field differ across applications, and many systems do not incorporate national data standards such as the NIEM. The disparity across data architectures and lack of standardization poses challenges to information sharing.

2.6 Information Sharing Architecture

The current state of information sharing is very limited across agencies within a county, circuit and district. Many agencies have standalone siloed systems that meet their specific functional needs but are not architected to facilitate information sharing.

Notably, several initiatives have been undertaken to advance the information sharing vision, including:

- The Prosecuting Attorney's Council has deployed a system known as Tracker across 41 Circuits for the District Attorneys. Tracker enables District Attorneys to share case information.
- Some local jurisdictions, Gwinnett County, Cordele Circuit and others have implemented information sharing solutions at the county and circuit levels.
- The Georgia Department of Corrections has begun to develop services to enable automated exchange of information.
- The Clerk of Superior Court uses the Georgia Superior Courts Clerks Cooperative Authority (GSCCCA) network to allow the Clerks to communicate in a limited manner as related to criminal data.

Due in part to system architecture limitations noted above, the vast majority of criminal justice agencies lack automated capabilities to enable cross-domain information sharing. Information is shared and transferred manually, via phone, fax, email and postal mail. When information is received, it is manually entered into the system of the receiving agency. This process is time consuming, resource intensive and prone to input errors.

2.7 Security Architecture

Security applied to current information sharing processes is highly varied, and in some cases, may not meet privacy and security requirements of the State. No enterprise-based security infrastructure or standards-based security approach has been implemented. In many instances, the sharing is based on an agency providing members of other agencies access to its case management or records management system. In such cases, the application security controls reside within the case management or records management system. In other instances, while network security is afforded through the use of the Internet with secure Virtual Private Network (VPN) tunnels for information transfer, data security measures are not employed.

Some reasons for the lack of security are:

- Lack of knowledge and/or awareness of available security features
- Lack of information regarding standards and the work that has been conducted by the Global Security and Privacy group and others
- Lack of technical resources

It is evident that the adoption of an enterprise based security infrastructure and approach based on standards will enable all participants to share information in a secure and safe manner and meet the privacy and security requirements of the State of Georgia.

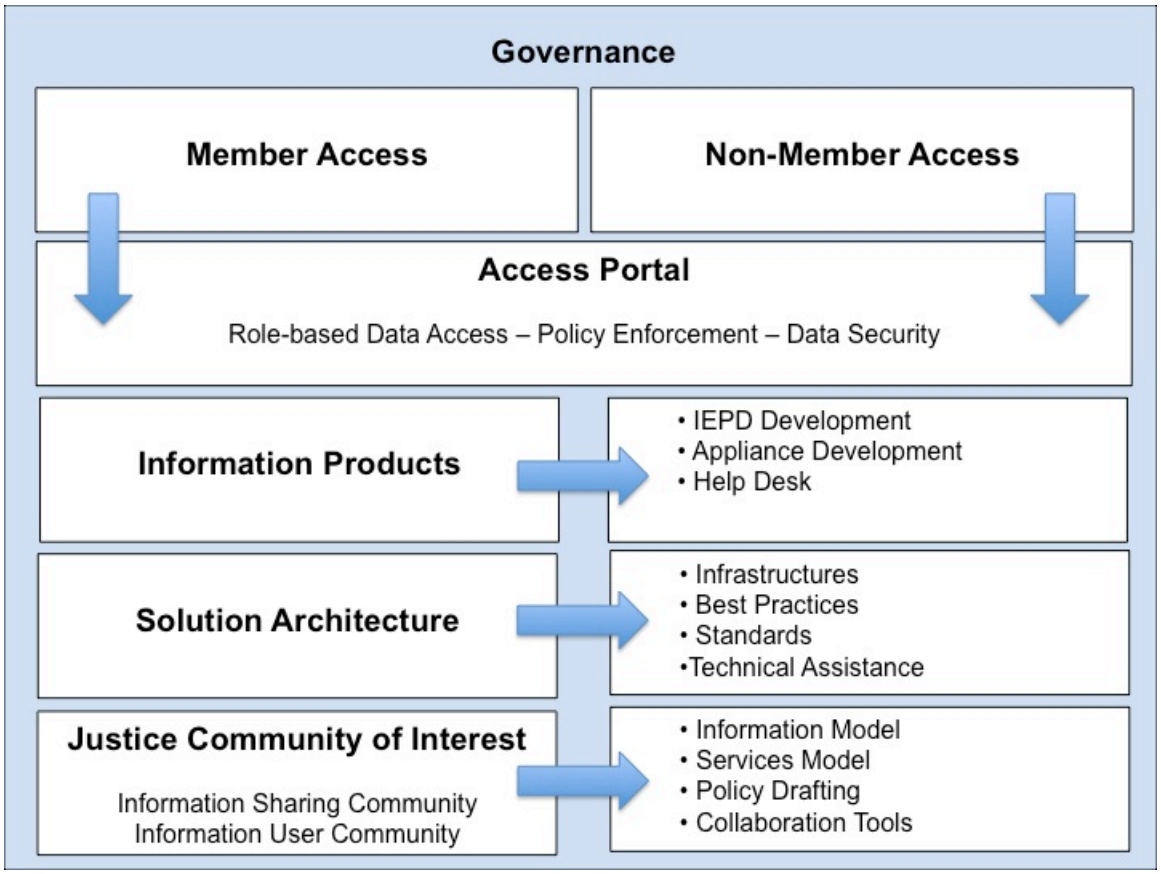
3 GeorgiaJDX Solution Architecture

GeorgiaJDX is an innovative concept based on the tenet that the key to more efficient and informed decision making lies in collaborating to achieve quality, integrated data at the source (i.e., local) level. A combination of technology, processes and governance allow this sharing infrastructure to be established and maintained.

Until recently, fully automated “data exchanges” could only occur using integrated records management and case management systems. This approach required a single, complex and expensive solution architected to meet the myriad specific and diverse needs of law enforcement, prosecution, courts and corrections agencies. With the advent of Service Oriented Architecture (SOA) and national standards for data exchange, the need for a single monolithic system meeting the needs of all agencies is eliminated, thus enabling agencies to leverage their existing technology investments and streamline data sharing implementations. The proposed GeorgiaJDX approach, which is based on the DOJ Office of Justice Programs Justice Reference Architecture, leverages SOA and national standards such as NIEM to create an information architecture solution aimed at enabling all stakeholders to share data seamlessly while retaining control of their individual business processes, applications and data.

As depicted in Figure 2, the GeorgiaJDX infrastructure comprises governance, users, technology and processes.

Figure 2: GeorgiaJDX Information Sharing Model



Components of the GeorgiaJDX Information Sharing Model include:

- **Governance** – Effective governance is essential to successfully implementing and managing the relationships, processes and systems comprising the Georgia JDX Information Sharing Environment. Various committees of the Governance Board render decisions on policies, information exchanges, business services, collaboration tools, etc. Section 5 discusses a proposed governance structure.

- **Justice Community of Interest** – The Justice Community of Interest comprises the Information Sharing Community and the Information User Community. The Information Sharing Community includes agencies that share and utilize information for operational and tactical purposes. Member agencies control their own data elements, decide what data is shared and sit on Governance Board committees. Members of the Information

User Community utilize information for strategic purposes such as strategy decisions and are not represented on Governance Board committees.

- **Portal** – The access portal provides Justice Community of Interest users access to information artifacts based on their defined access rights.

- **Solution Architecture** – The Solution Architecture provides the technical framework for all agencies to share information within a county and circuit and across counties and circuits. The remainder of this document discusses the Solution Architecture in detail.

- **Information Products** – Common products and assets will be developed once and shared by all members of the GeorgiaJDX community, thus promoting reuse and cost-effectiveness. Examples of Information Products are Information Exchange Packages (IEP) such as the Arrest Warrant, Daily Jail Report and Sentencing packages.

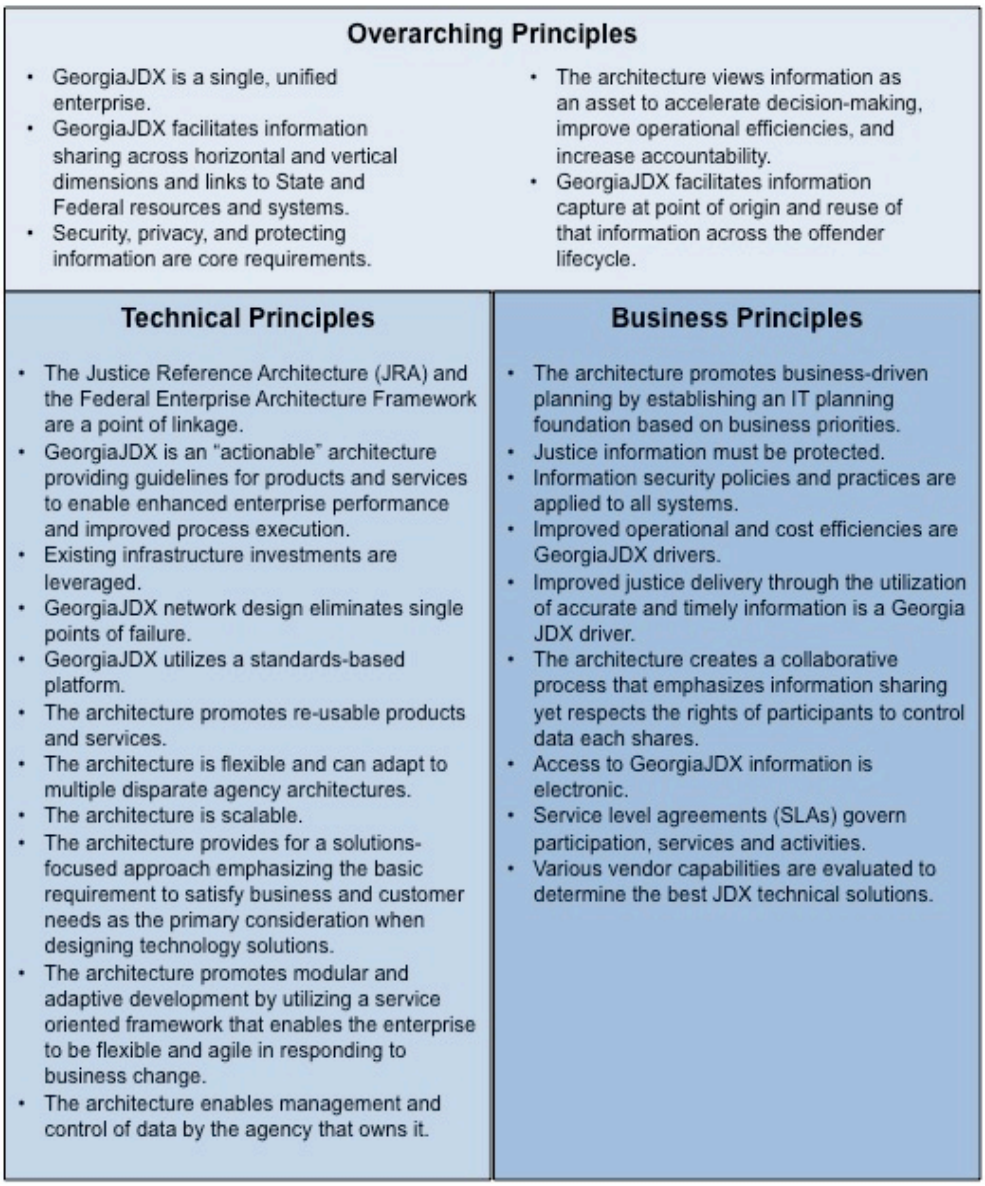
The GeorgiaJDX Solution Architecture is based on a set of architecture principles derived from the Justice Reference Architecture developed by the Global Infrastructure/Standards Working group and the SOA Reference Architecture developed by the Organization for Advancement of Structured Information Standards (OASIS). The three dimensions of architectural principles supporting the development of the GeorgiaJDX Solution Architecture, as presented in Figure 4, include:

- **Overarching Principles** – Overarching principles reflect the overall tenets of the GeorgiaJDX architecture. They represent the focal point for agencies' information sharing-focused IT initiatives and influence foundational elements for agencies to develop and enhance their agency applications. By adhering to these overarching principles, agencies will be able to develop measures to assess IT performance and ensure adherence to the GeorgiaJDX vision and objectives.

- **Business Principles** - These principles represent the business goals supported by the GeorgiaJDX architecture. As previously discussed, the architecture and the technology must be robust, agile and scalable to support the business goals of GeorgiaJDX.

- **Technical Principles** - These principles represent the technology tenets that drive the selection of the components for the GeorgiaJDX architecture. While GeorgiaJDX is a virtual environment, its physical infrastructure and access will include IT elements leveraged across the Georgia justice community. A set of best practices for the technical components of GeorgiaJDX reflects industry practices for similar types of environments. This set of technical principles refers to existing efforts in information sharing across multiple states and is based on input from multiple GeorgiaJDX stakeholders.

Figure 3: GeorgiaJDX Architecture Principles



The architecture of the GeorgiaJDX Information sharing Environment (G-ISE) is based on the defined needs of GeorgiaJDX community participants and leverages the architectural models and frameworks developed by the National Center for State Courts (NCSC), the Justice Reference Architecture (JRA) developed by the Global Infrastructure/Standards Working Group (GISWG) and the OASIS Reference Architecture. This architecture framework is service based to allow GeorgiaJDX to rapidly implement information sharing capabilities, to be flexible and agile and to adapt to changing business needs quickly and efficiently.

The GeorgiaJDX team visited a number of counties and circuits to understand the current environment, challenges and needs of the participants. A review was conducted of other states' best practices and of work performed by national organizations such as the GISWG, NCSC, and others. The team also reviewed and incorporated The Court Technology Framework developed by the National Center for State Courts into the G-ISE architecture. The G-ISE is designed to support the following functional objectives:

- Provide an environment for the participants in the GeorgiaJDX to exchange information in a secure and reliable manner

- Provide an environment in which participants can make information available for other participants and where such information can be searched in a secure and reliable manner, including information products made available to external entities

- Provide an execution context through which the participants can access and utilize common services. An execution context is a set of Infrastructure components, processes and policy assertions that are a part of the interaction between the provider and consumer of business services.

- Accommodate varying capabilities of participants

- Provide a communication infrastructure that provides connectivity between the various counties, between the counties and the circuits, and between the counties and state level entities

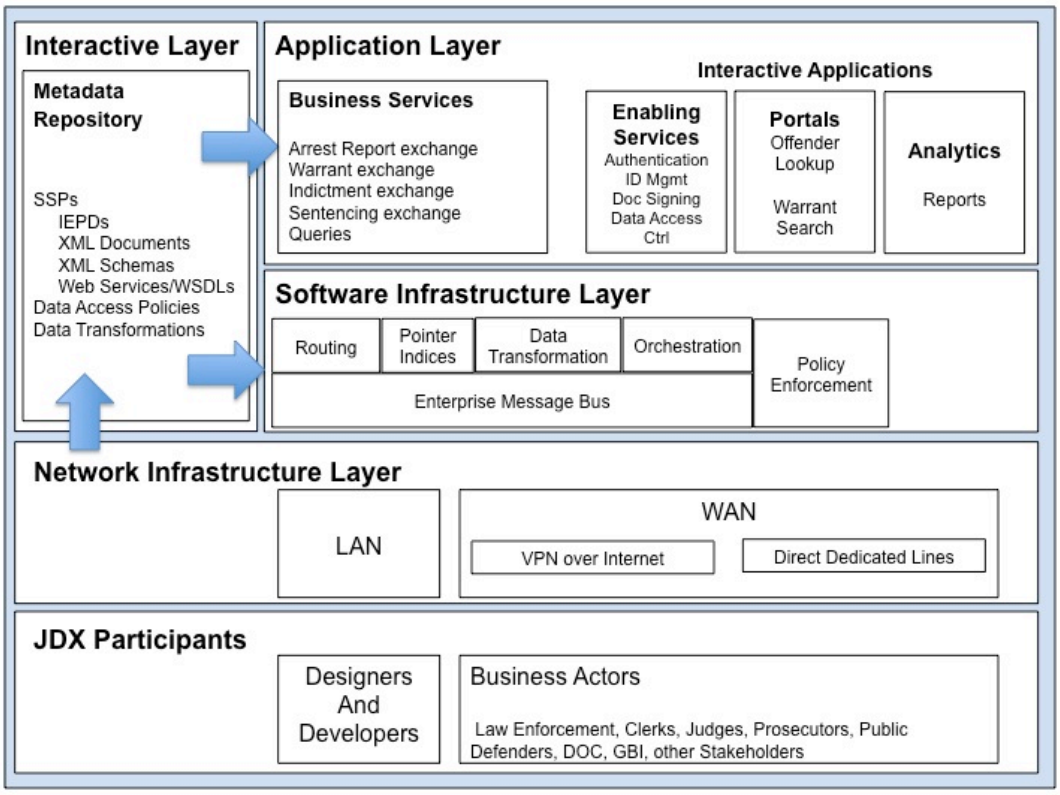
The remainder of this section describes the complex and multi-dimensional G-ISE architecture. It must be viewed from multiple perspectives to be completely understood, and is thus presented as a *Functional* view*,* a *Logical* view and a *Physical* view. Each view provides a perspective from a different dimension and is described and diagrammed below.

After a discussion of the three perspectives, scenarios are presented that describe the manner in which the G-ISE architecture supports the information exchanges within and across counties, within and across circuits, and between the counties and the State. This chapter concludes with a discussion of the manner by which the G-ISE supports the Justice Reference Architecture described previously in this document.

3.1 Functional View

The Functional View provides a view of the G-ISE architecture from an operational perspective. It discusses the different functional components of the architecture and describes what each component provides. Figure 4 depicts a functional view of the G-ISE architecture.

Figure 4: G-ISE Architecture - Functional View



Each layer of the Functional View of the G-ISE architecture – the Interactive Layer, the Application Layer, the Software Infrastructure Layer and the Network Infrastructure Layer – is described below.

3.1.1 Interactive Layer

The interactive layer is a metadata repository containing artifacts to be utilized by the members of the GeorgiaJDX community to share information. It is expected that members wanting to utilize artifacts will have access to these artifacts and will be able to use them to exchange information with other agencies within a county, circuit, across circuits and with state agencies.

The metatdata repository houses the following:

- **Service Specification Packages –** Service Specification Packages (SSPs) document the conceptual, logical and physical models of a service. An SSP comprises a set of documents, diagrams, models, and templates that provide a comprehensive view of the capabilities and business and technical requirements of a service and a blueprint for service implementation. SSPs describe information exchanges, connection methods (typically Web Services) and security specifications.

  Service Specification Documents – Service Specification Documents (SSDs) document the capabilities made available through a specific service by providing service providers all information necessary for exposing a service in a consistent, interoperable manner and service consumers all information necessary for consuming that services. SSDs include service descriptions and service interface descriptions. Service descriptions comprise all aspects of a service not directly tied to the physical implementation or service interface. Service descriptions include NIEM-conforming Information Exchange Package Documents (IEPDs) that describe the conceptual, logical and physical models of each exchange. Service interface descriptions describe the physical

implementation and define what an implementer uses to build executable software that interacts with the service to enable information exchange.

XML Documents and Schemas - XML is a set of rules for encoding documents electronically, with design goals of emphasizing simplicity, generality and usability over the Internet. An XML document is a collection of data represented in XML. An XML schema describes the structure of an XML document, including elements and attributes and their respective data types and default and fixed values.

Web Services – Web services provide platform-independent protocols and standards for exchanging data between applications in SOA solution architectures. Web services are defined by Web Services Description Language (WSDL). WSDLs are XML formats for describing network services as sets of endpoints operating on messages. WSDLs are extensible to allow description of endpoints and their messages regardless of what message formats or network protocols are used to communicate.

- **Data Access Policies** - The metadata repository contains rules governing access to data by members at various organizational levels. These policies will be stored in a form that can be utilized by the software Infrastructure layer to limit access to the members of the GeorgiaJDX community.

- **Data Transformation Rules** - The metadata repository contains data transformation rules that will be implemented to transform data and exchange data between agencies' systems. Data transformation maps and converts data from the format of the source system or application to the format of the destination system or application

3.1.2 Application Layer

The second functional layer of the G-ISE architecture is the application layer. This layer hosts the services and functions that provide business value to the members of the

GeorgiaJDX community. Components in this layer utilize the network infrastructure layer and the software infrastructure layers to deliver business and enabling functionalities to GeorgiaJDX participants. Below are descriptions of the three primary components of the application layer.

- **Business Services** - Business services are applications that include one or multiple services providing a specific business value to users in the form of information. Examples of business services are exchanges, such as the Arrest Report, Indictment, Warrant and Sentencing exchanges, as well as queries, such as CJCC queries to the GBI computerized criminal history repository. As is discussed in the Logical View of the G-ISE architecture, business services can reside at the state or local level to accommodate the needs of small, medium and large counties.

- **Enabling Services** - Enabling services do not provide direct business value to GeorgiaJDX but support business services in providing business value. Examples of enabling services include identity management, document signing, authentication and data access control.

- **Interactive Applications** – Interactive applications enable GeorgiaJDX members to access information and information products. Interactive applications include Portals and Analytics. Portals enable members to conduct federated queries and searches across the G-ISE architecture. Offender Lookup and Warrant Search are examples of federated queries initiated through a portal. Analytics enable members to access pre-defined reports or to structure on-the-fly reports indicating patterns and trends.

3.1.3 Software Infrastructure Layer

The software infrastructure layer encapsulates six basic functions critical to the operation of the G-ISE. This layer contains the components that route messages, enforce policies and access control, transform data and conduct orchestration activities. The key components of the software infrastructure layer and the functions each performs are described below.

- **Enterprise Message Bus** - The enterprise message bus allows communications to occur between multiple applications by routing exchange information from senders to receivers. An important capability of an enterprise message bus is the ability to provide guaranteed message delivery to ensure the flow of information is automatically resumed when a participant's system becomes available again after an outage. When delivery cannot be completed within a specified period of time, the enterprise message provides alerts and warnings. The enterprise message bus also permits the replay of messages when necessary. The message bus supports the following four functions:

  Routing – GeorgiaJDX information flow is enabled by rules-based routing engine that routes messages from one participant to one or multiple participants based on the rules for each specific message.
  The sender hands the message over to the enterprise message bus, which assumes responsibility for delivering the message to recipients based on pre-defined message routing rules. Multiple destinations for a given message can be defined by configuring an appropriate message routing rule. Rules are also defined to enable error correction. For example, the requirements definition process may identify a requirement to notify the Sheriff's Office initiating a warrant request if/when the Clerk makes a spelling change to the offender's name. A rule can be defined to provide notification of the change to the Sheriff's Office. The Clerk does not directly access the Sheriff's system to make the spelling change, but rather the Sheriff's Office receives an automated notification and can apply its own internal change management policies. Rule-based routing is particularly useful when dealing with mechanized flows that require data transformation or multiple intermediate steps (see Orchestration below).

  The enterprise message bus also supports the flow of information through the use of the Publish/Subscribe model. Entities originating a message assign a topic or subject to the message. Entities wishing to receive messages of particular content subscribe to specific topics. The

enterprise message bus assumes responsibility for delivering the message to the correct entities.

Pointer Indices - Pointer indices are incorporated in the G-ISE architecture to improve performance. Due to the large number of expected members of the GeorgiaJDX community, a simple information search and discovery approach would overwhelm the network and software infrastructure when the search is federated across multiple agencies' systems. Pointer indices provide an efficient mechanism for search and discovery by periodically indexing key pieces of searchable information. These indices will contain information about where to locate records that meet the specified criteria. To preserve the privacy of the information being disseminated, pointer indices will contain the minimal amount of information required to locate the information in the host system, and will be updated on a periodic basis utilizing the publish/subscribe and the guaranteed message delivery capabilities of the enterprise message bus.

Data Transformation - The data transformation component transforms messages to render them NIEM-conforming so receiving entities all receive the same message in the same standards-based format.

Orchestration - The Orchestration component sequences how multiple services are executed to satisfy a business function. For example, if a Warrant Search needs an identifier from one system and this identifier is then used to extract data from another system, the orchestration component sequences both services to enable the user to extract and view data.

- **Policy Enforcement** - The policy enforcement component provides an execution context to enforce the information and service access policies registered with the repository. (An execution context is a set of technical and business elements that

form a path between those with needs and those with capabilities and that permit service providers and consumers to interact.) Policy enforcement is applied by the components of the enterprise message bus and business services.

3.1.4 Network Infrastructure Layer

The primary function of the network layer is to provide secure and reliable connectivity between the various entities and systems participating in GeorgiaJDX. The network infrastructure must ensure the messages are delivered in a secure manner free from interception and eavesdropping. As discussed in Section 2.0, the communications infrastructure between entities in counties and circuits is not robust. Hence, the network infrastructure layer must support multiple communications methodologies to accommodate the varying needs of participating agencies.

The network infrastructure layer supports both Wide Area Network (WAN) and Local Area Network (LAN) connectivity. Each participating agency will determine the type of connectivity to utilize. The various LAN and WAN configurations are described below.

- **Local Area Network** - Co-located entities may utilize a local area network to communicate with each other. For instance, in a jurisdiction with a countywide LAN, Sheriff's Offender Management System and the County Clerk's Case Management System may use this LAN to share information.

- **Wide Area Network** – A Wide Area Network is a network configuration enabling interactions between geographically dispersed entities or entities that are not co-located. The network infrastructure layer supports types of WAN connectivity:

  Dedicated Lines – Dedicated lines are direct connections between entities that provide a secure conduit for messages. Routers are installed at the end points to map shared network resources into each other's networks. Dedicated lines are costly and require careful monitoring, so should be used only when the local policies preclude the flow of data over the Internet, even when encrypted.

Virtual Private Network (VPN) over the Internet – VPN over the Internet is a preferred method of communication between the members of the GeorgiaJDX community. VPN is a cost-effective means to realize a WAN. VPN routers encrypt messages that flow over the public Internet. VPN routers at the participating entities are paired with one another with encryption keys to ensure only properly configured routers can decode messages. This mechanism avoids the need for dedicated lines and often, a single VPN router can be configured to provide peer-to-peer connections between multiple partners.

Table 2 presents proposed network connectivity for small counties participating in GeorgiaJDX. Table 2 presents proposed network connectivity for medium and large counties.

Table 2: Proposed Network Connectivity for Small Counties

	LAN	VPN Over Internet	Dedicated Lines
Clerks and Sheriffs	If co-located	If not in same Data Center	If not in same Data Center and if local policies require the use of dedicated lines
Clerks and Prosecutor (Tracker)	If co-located	Always	Never
Clerks and State	If CMS is hosted at the State	If CMS is hosted at the County	Same as above
Clerks and Other Counties	Never	Always	Same as above
Clerks and Portals	Never	Always (Browser-based)	Never
Clerks and Analytical Products	Never	Always (Browser-based)	Never

Table 3: Proposed Network Connectivity for Medium and Large Counties

	LAN	VPN Over Internet	Dedicated Lines
Clerks and Sheriffs	If co-located	Preferred	If local policies require the use of

			dedicated lines
Clerks and Prosecutor (Tracker)	If co-located	Always	Never
Clerks and State	Never	Always	Never
Clerks and Other Counties	Never	Always	Never
Clerks and Portals	Never	Always (Brower-based)	Never
Clerks and Analytical Products	Never	Always (Browser-based)	Never

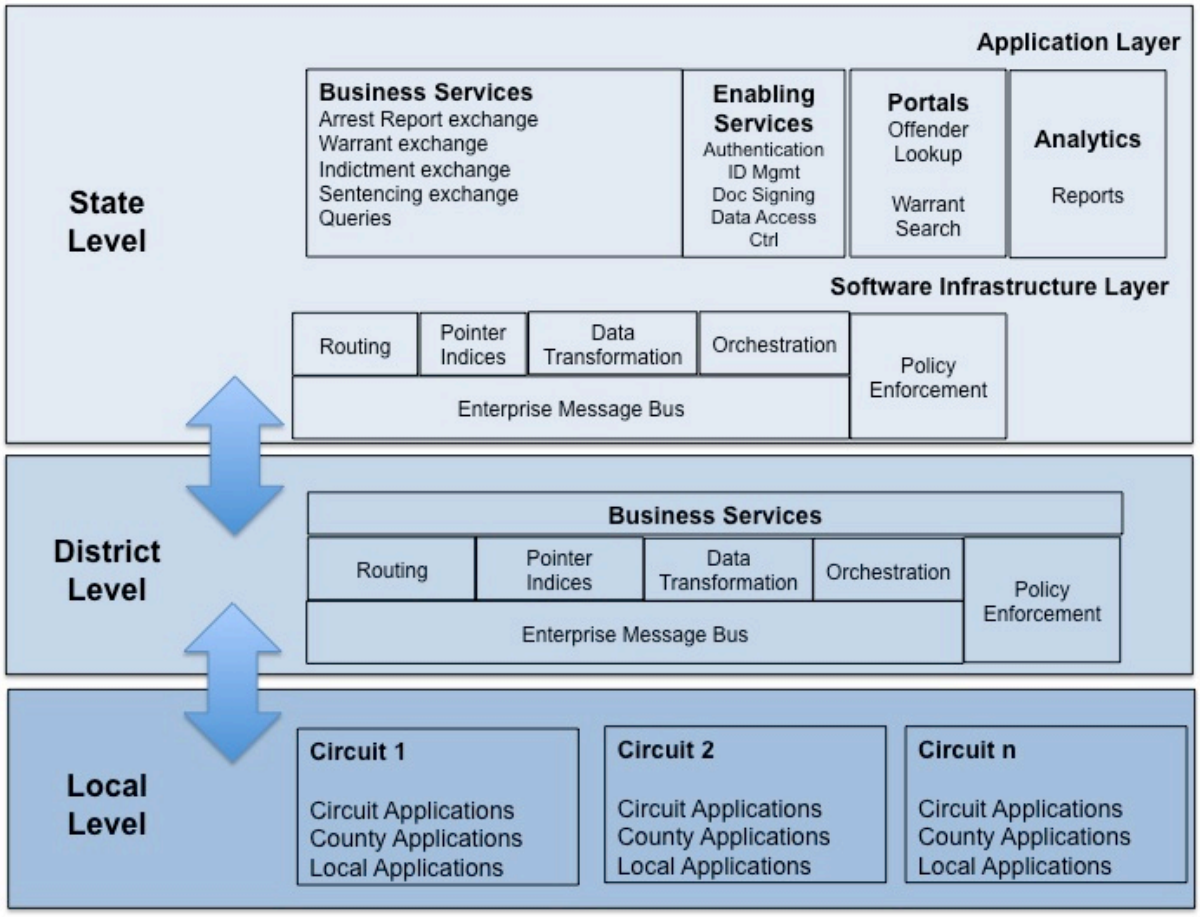
3.2 G-ISE Architecture – Logical View

The Logical View provides a geographical perspective of where the G-ISE architecture components will be deployed. The Logical view comprises the State level, the District level and the County/Circuit level. Components deployed as part of GeorgiaJDX should reside primarily at the District level. Georgia comprises ten districts, each composed of multiple circuits and counties. Deploying architecture components at the district level leverages hardware assets and enables circuits and counties too small to fund infrastructure to participate in GeorgiaJDX. This section describes how information sharing will function within a county or circuit, between counties or circuits, and between the counties, circuits and state entities.

The proposed architecture allows members of the GeorgiaJDX community to communicate with each other at the District level while allowing them to utilize applications that may reside at the Central level to communicate across Districts and share information across Georgia. The benefit of this approach is that it allows the model to scale very easily since all transactions are directed to the appropriate District rather than passing through a central point. The local transactions occur at the District level and the ones that require access to multiple Districts occur at the State level. As previously noted, this architecture enhances scalability since the traffic and the transactions can be directed to the appropriate District.

The State, District and Local levels are depicted in Figure 5 and discussed in greater detail below.

Figure 5: G-ISE Architecture - Logical View



3.2.1 State Level

At the State level is a shared layer for all members of the GeorgiaJDX community. This shared layer has functionality that can be shared and utilized by all members. The application layer described in section 3.1.2 and the software infrastructure layer described in Section 3.1.3 comprise the shared functionality layer at the State level.

As described in Section 3.1.2, the application layer consists of the following components:

- Business Services
- Enabling Services
- Interactive Applications, including Portals and Analytics

As described in Section 3.1.3, the software infrastructure layer consists of three primary components and multiple sub-components:

- Enterprise Message Bus

Routing
Pointer Indices
Data Transformation
Orchestration

- Identity Resolution
- Policy Enforcement

3.2.2 District Level

The District level is a subset of the State Level. Some components of the Application Layer and Software Infrastructure Layer are hosted at the District level. This design enables redundancy in the infrastructure architecture, which facilitates configuration of backup and failover solutions. The design also provides scalability by enabling other Districts to be easily added as additional counties and circuits become prepared to join the G-ISE. The primary difference between the State and District levels is the absence of enabling services, central portal applications and reporting and analytics components from the application layer at the District level. Only the application layer and the software infrastructure layer are duplicated at both the State and District levels.

3.2.3 Local Level

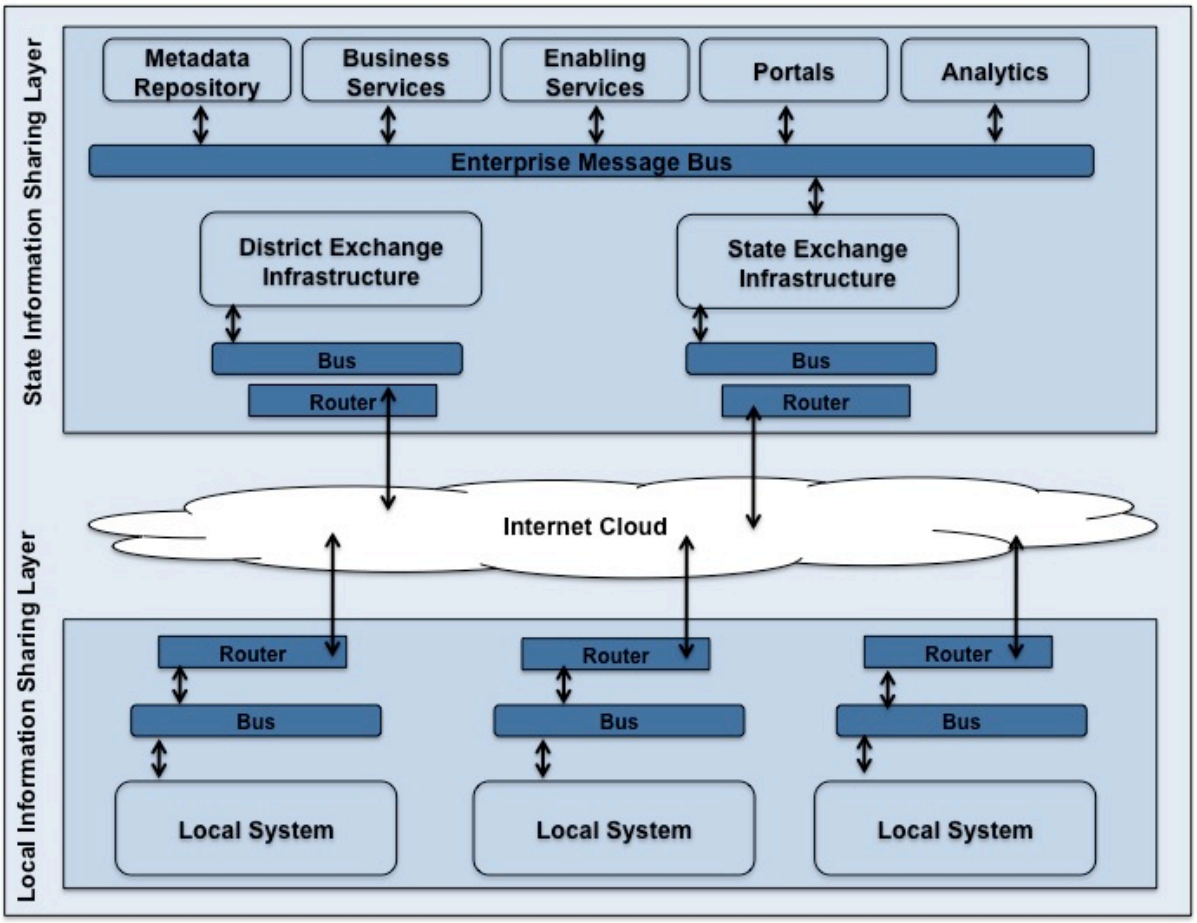
At the Local Level are all Circuit, County and City entities. The case management and records management systems that support the daily operations of the Circuit, County and City agencies are deployed at the local level of the G-ISE architecture. Such agencies within a District communicate and share information with each other through architectural components deployed at the District level. These local agencies can communicate with other Districts through components deployed at the State level.

3.3 G-ISE Architecture – Physical View

The Physical View depicts and describes the positioning of the hardware, applications and services comprising the G-ISE architecture. This perspective discusses the physical implementation of the technology and software components and where each resides – at the State/District level or at the County/Circuit level. This perspective provides insight into the manner in which the physical components are deployed and how the capabilities they enable operate. As previously noted, the current technical infrastructure in many of the counties is inadequate to support robust information sharing. The G-ISE architecture supports the needs of

all counties regardless of the state of their current information sharing infrastructures. As depicted in Figure 6, the G-ISE architecture is physically deployed in two layers, the State Information Sharing Layer and the Local Information Sharing Layer. While some components of the Application Layer and Software Infrastructure Layer are hosted at the District level as noted in Section 3.2.2, the physical deployment of the hardware to support those components may be either at a state data center or at a regional facility depending on the best case cost scenario for availability of a suitable facility and support resources. Figure 6 assumes physical deployment at a state facility.

Figure 6: G-ISE Architecture, Physical View



3.3.1 State Information Sharing Layer

The State Information Sharing layer components reside at a state-level site such as a state data center and support all members of the GeorgiaJDX community. The Software Infrastructure, Interactive and Application layer functions of the State and District levels of the G-ISE Architecture Logical View are performed using the components of the State

Information Sharing layer. The hardware required for implementation of State Information Sharing layer functions are detailed in Table 4.

Table 4: State Information Sharing Infrastructure

Type	Function	Hardware Required
State Level Infrastructure (Software Infrastructure Layer)	Hosts message bus, policy enforcement, routing engine, data transformation and pointer indices	1 server
Metadata Repository (Interactive Layer)	Stores metadata, exchanges and services	Runs on server above
Business Services (Application Layer)	Stores business services at the State level	Runs on server above
Enabling Services (Application Layer)	Stores enabling services at the State level	Runs on server above
Reporting & Analytics (Application Layer)	Stores the applications and databases to support State-level Reporting and Analytic functions	Runs on server above
Portal Applications (Application Layer)	Stores the central applications including those supporting federated queries across all members of the GeorgiaJDX community. Query examples are Offender Lookup and Sentencing Exchange.	Runs on server above

3.3.2 Local Information Sharing Layer

This Local Information Sharing layer consists of the G-ISE components needed to support information sharing between the records management and case management systems of City, County and Circuit-level entities. Local Information Sharing layer hardware requirements are shown in Table 5.

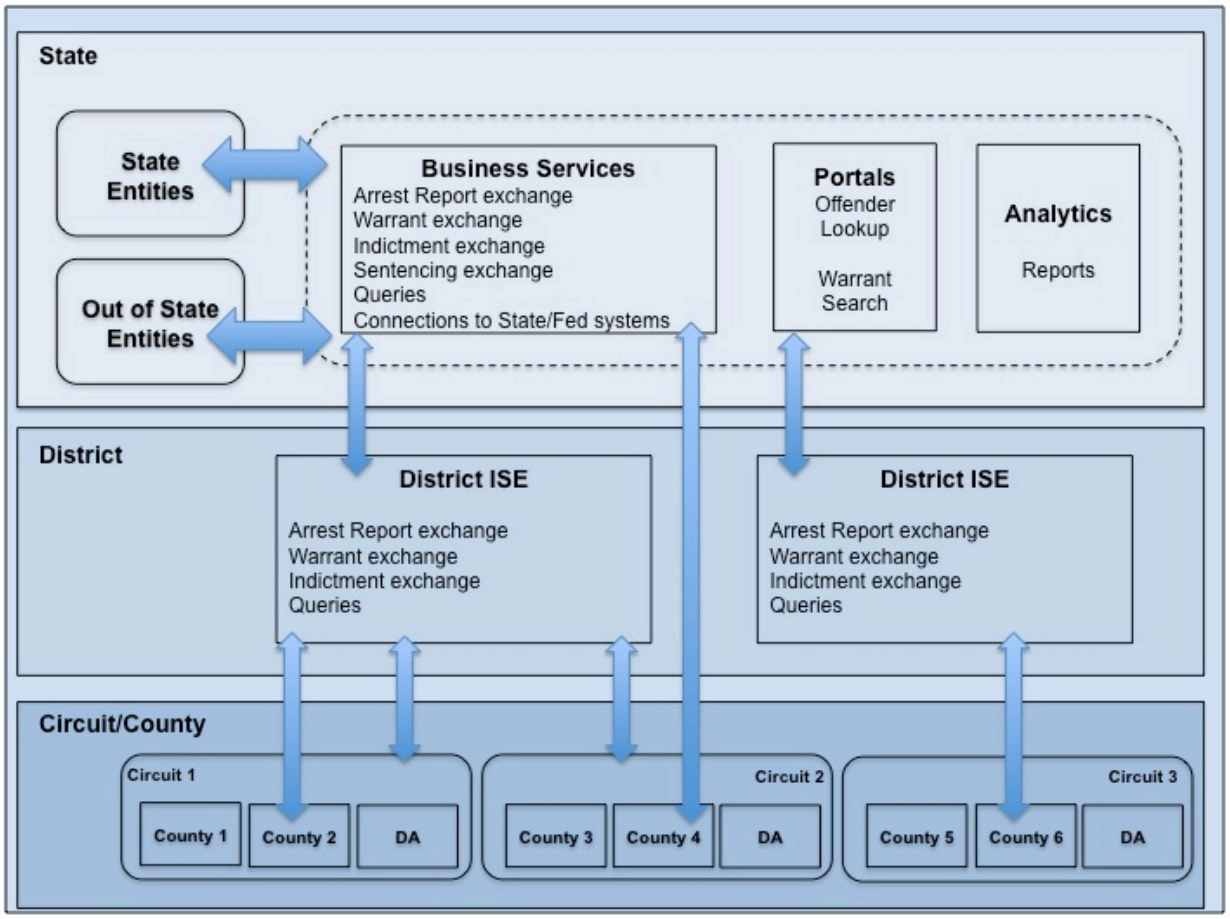
Table 5: Local Information Sharing Infrastructure

Type	Function	Hardware Required
District Level Exchange Infrastructure (Software Infrastructure Layer)	Hosts message bus, policy enforcement, routing engine, data transformation and pointer indices	1 server
Business Services (Application Layer)	Stores the business services at the District level	Runs on server above

3.4 Information Sharing Across Organizational Boundaries

The section discusses how members of the GeorgiaJDX community share information with other members as well with State and Federal exchange partners. Figure 7 presents a high level view of how the State, District and Local infrastructures interact to enable information sharing.

Figure 7: Information Sharing Across Organizational Boundaries



The State level, which is discussed in G-ISE Logical View, is the single point of contact from the City, County and Circuit members to State and Federal entities. The application level business services, including the Arrest Warrant, Sentencing and Disposition exchanges, define how information is forwarded to State agencies such as the Georgia Department of Corrections and Georgia Bureau of Investigations. The use of such standards-based exchanges ensures information is pushed to these agencies' systems in a common format and any changes required to accommodate legislative or similar policy mandates are done in a single location. This centralization also facilitates maintenance of the exchanges.

The GeorgiaJDX members at the County/Circuit level can either share information using either Local Area Networks or Wide Area Networks. If the agencies are co-located LAN, that LAN can

be utilized for information sharing. If they are not co-located, the District Exchange Infrastructure can be used to exchange information. If the District Exchange Infrastructure is utilized, use of a WAN with either VPN over Internet or dedicated lines is required. VPN over Internet is strongly recommended unless prohibited by legislation or policy issues. The VPN approach can be utilized to share information across the Circuit and between all Circuits in a District.

When a County/Circuit-level agency exchanges information with the State and/or Federal exchange partners, the information is passed from the agency to the District Exchange Infrastructure in the manner described above. The District Exchange Infrastructure communicates with the State Level Exchange Infrastructure. The State Level Exchange Infrastructure receives the information and pushes it to the State/Federal entities. Any information received from State/Federal entities is pushed down to the District Exchange Infrastructure and to the circuits, counties and cities connected to it. The G-ISE architecture accommodates small agencies with no LAN/WAN capabilities by enabling access via the portals at the application layer of the State Level Exchange Infrastructure. The only requirement for such access is a computer with Internet access. This functionality enables all agencies to participate in GeorgiaJDX without investing in technology and communications infrastructure.

Any information exchange between counties or circuits in different districts utilizes the State Level Exchange Infrastructure. The information to be exchanged is forwarded from the county/ circuit member to the State Level Exchange Infrastructure via the District Exchange Infrastructure. The State Level Exchange Infrastructure forwards the information to the appropriate District Exchange Infrastructure and from there to the appropriate county/circuit member in that District.

3.5 Conformance with Architecture Standards

The G-ISE architecture leverages best practices in the public sector as well as accepted and national data architecture and exchange standards. One such standard is the Justice Reference Architecture developed using the Service Oriented Architecture Reference Model developed by the Organization for Structured Information Standards (OASIS). OASIS is a nonprofit, international consortium whose goal is to promote the adoption of product-independent standards. OASIS works to bring together competitors and industry standards

groups with conflicting perspectives to discuss using Extensible Markup Language (XML) as a common language that can be shared across applications and platforms. The JRA standard also utilizes NIEM, the use of which is mandated as a special language in all information sharing grant funding provide by the Bureau of Justice Assistance and the Department of Homeland Security.

The Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee (FAC) and advises the U.S. Attorney General on justice information sharing and integration initiatives. Global was created to support the broad scale exchange of justice and public safety information. It promotes standards-based electronic information exchange to provide the justice community with timely, accurate, complete, and accessible information in a secure and trusted environment. Global is a "group of groups," representing more than 30 independent organizations, spanning the spectrum of law enforcement, judicial, correctional, and related bodies. Member organizations participate in Global with a shared responsibility and shared belief that, together, they can bring about positive change by making recommendations and supporting the initiatives of the U.S. Department of Justice.

The key principles of the JRA[3] are listed as follows:

1. Independence of Information Sharing Partners
2. Diversity of Data Source Architecture
3. Alignment with Best Practices and Experience
4. Agility
5. Scalability
6. Re-Use and Sharing of Assets

Below is how the JRA Principles are implemented in the G-ISE architecture:

- **Independence of Information Sharing Partners** - Members sharing information using the G-ISE architecture are independent organizations with a business need to exchange information. This principle influences the manner in which members make their services available to each other.

[3] Justice Reference Architecture Specification, Ver 1.7

Realization - In broad terms, this independence is realized by making business functionality available through service interface, by isolating the implementation from the interfaces, and careful design of the services.

- **Diversity of Data Source Architecture** - The members of the GeorgiaJDX community are vastly different in size, have differing levels of expertise, and utilize a variety of IT products. The architecture supports the heterogeneous nature of the Information Sharing Environment.

  Realization - This principle is realized by utilizing open, industry-standard communications mechanisms and well-designed interfaces that delink implementation and interface. The architecture also supports varying capabilities by providing common services accessible by all GeorgiaJDX participants.

- **Alignment with Best Practices and Experience** – To efficiently utilize the available financial resources and to avoid the pitfalls of past implementations, the architecture incorporates proven industry best practices.

  Realization - To realize this principle in practice, the members and system designers must be continuously exposed to ongoing efforts in implementation and evolvement of the G-ISE. The architecture calls for creation and active engagement of user groups, knowledge bases, and collaboration zones to promote knowledge dissemination.

- **Agility** - The architecture enables member agencies to evolve their systems to meet their internal operational needs. Changes to individual systems can be effected while preserving existing information sharing.

  Realization - Adherence to well-defined and documented interfaces, use of standards-based implementations, message routing abstractions and rule-based data transformations and isolation of core functionality into the infrastructure enables realization of the Agility principle.

- **Scalability** - The architecture's design principles apply to member agencies of all sizes and capabilities.

  Realization - The architecture addresses this principle through the use of consistent interfaces, consistent software infrastructure and the ability to support multiple modes of interactions. In addition, the architecture encapsulates certain core services and functionality into a common infrastructure available to all members.

- **Reuse and Sharing of Assets**: The architecture fosters reuse of information exchanges and system interfaces.

  Realization: The architecture provides and adheres to carefully defined information exchange models.

  - Exchanges are defined to accommodate the needs of all participants rather than being tailored for specific endpoints.
  - Exchanges are implemented to the maximal data models. A maximal data model is designed to support exchanges of a specific type between different sets of stakeholders. Such data models contain the 'sum' of the data elements required by each stakeholder system.
  - The architecture also supports a searchable repository to house information exchange and service specifications.

3.5.1 Conformance with JRA Execution Context Guidelines

This sub section discusses the JRA Execution Context Guidelines[4] and the manner in which the G-ISE architecture supports these guidelines. These guidelines form the basis on which a key component of the G-ISE, namely identity management, is manifest. The term *Execution Context* refers to Infrastructure components, processes and policy assertions that are a part of the interaction between the provider and consumer of business services. The guidelines are summarized as follows:

[4] JRA Execution Context Guidelines, Version 1.0

- **Reachability** - The consumers or users of business services can interact with the service providers through communications channels.

  Realization - This principle is realized in the G-ISE by;

  - The creation of the G-ISE in which state-wide services and portals are hosted
  - The Network Infrastructure Layer that facilitates communications between the consumers and the providers of business services
  - The creation of regional exchanges to isolate network traffic for inter-county information sharing

- **Willingness** - The term *willingness* reflects the scope and nature of the interaction between the consumer of a business service and the provider of the service. Willingness of a business service to interact with a consumer is dependent on a variety of factors, including:

  Network Security: Network security refers to the manner in which privacy of the interaction is protected.

  Realization - Service providers in the G-ISE architecture support listeners only on channels on which the network infrastructure is able to guarantee privacy.

  Identity Provisioning and Management and Shared Security Infrastructure: The providers of business services are assured of the identity of the user, system or application that initiates an interaction with the service.

  Realization: The G-ISE architecture utilizes Global Federation Identity and Privilege Management (GFIPM). The G-ISE shall host Identity Provider (GFIPM – IP). The architecture also requires all business service providers in the G-ISE to support GFIPM user assertions, when appropriate.

  Shared Policy Infrastructure - An additional element of the Willingness guideline is the availability of the following entities in the Infrastructure: Fine Grain Authorization, Authorization Policy, Policy Decision Points and Policy Enforcement Points.

Realization - G-ISE provides this functionality in the Software Infrastructure Layer. Specifically, the following design and runtime components are supported:

- **Fine Grain Authorization** – Fine grain authorization refers to authorization at the data element level.
- **Authorization Policy** - These policies govern access to information. These shall be implemented using XACMLXML Access Control Markup Language (XACML).
- **Policy Decision Points and Policy Enforcement Points** - These are common modules that shall be utilized by the business services to enforce the authorization policies.

- **Awareness** - The JRA Implementation guideline of awareness refers to the existence of infrastructure components that permit service consumers to seek out and discover service providers. This awareness covers the behavior and information models.

  Realization - The G-ISE architecture realizes this guideline through implementation of a service repository, defined in this document as the Metadata Repository.

- **Intermediaries**: The term *Intermediary* refers to the ability to receive requests from entities and submit requests on their behalf.

  Realization: The Software Infrastructure described above, with the Message Bus, provides extensive support for this functionality.

4 Action Plan

This section describes how the G-ISE solution architecture is deployed. The approach identifies and deploys "quick wins" and incrementally adds components and technology to the G-ISE architecture. This strategy positions the architecture to scale as members join the Information Sharing and Information Users communities. The action plan comprises three incremental phases to be undertaken in the short term (next six months), medium term (six months to one year and medium to long term (over one year). While approximate timeframes are assigned to each phase, the timeframes are not absolute and will evolve based on available funding and technical and operational readiness of agencies to participate. Table 6 below defines the actions, high-level tactics and suggested timeframes of each phase. Phase I, during which the foundational infrastructure is created and initial exchange implementations are accomplished, is described in greater detail in Section 4.1.

Table 6: G-ISE Deployment Action Plan

Actions	Tactics	Timeframes
Phase I		
Deploy basic technology infrastructure	Finalize governance structure Finalize and procure technology components Implement technology infrastructure	Short term (next 6 months)
Finalize, develop and deploy quick wins	Prioritize quick win exchanges and applications Define project management methodology and plan for development and deployment Develop and implement quick win exchanges and applications in selected circuits/counties Monitor performance of initial deployments	Short term (next 6 months)
Phase II		
Roll out quick win applications and exchanges to additional circuits/counties	Establish Program Management function Identify and prioritize Phase II participants Implement quick win exchanges and applications to Phase II	Medium term (6 months to 1 year, then ongoing)

Actions	Tactics	Timeframes
	participants using defined project management methodology Monitor performance of Phase II deployments	
Phase III		
Harden technology infrastructure	Monitor volume of participants joining the G-ISE environment and the impact on infrastructure and performance Identify points at which the architectural components need to be replaced or augmented to meet the additional demands on the G-ISE architecture Acquire and install identified components	Medium to long term (over 1 year)
Develop additional exchanges, applications and services based defined business goals	Identify and prioritize exchanges and applications based on business needs Work with vendors to develop and implement new applications and exchanges Monitor performance of all deployments	Medium term – long term (on-going effort)

4.1 Phase I Actions and Tactics

The actions and tactics of Phase I provide the core G-ISE foundation and infrastructure for GeorgiaJDX information sharing. Phase I scope incorporates the following assumptions:

- The initial infrastructure deployment supports ten circuits and 30 counties.
- Several information exchanges and applications have been identified and prioritized as quick wins. While exchanges and applications will be initially deployed on a deliberately limited basis, each will be developed according to JRA and NIEM standards so as to be deployable by other districts' circuits and counties over the life of GeorgiaJDX. These are described in the recommendations discussed below.

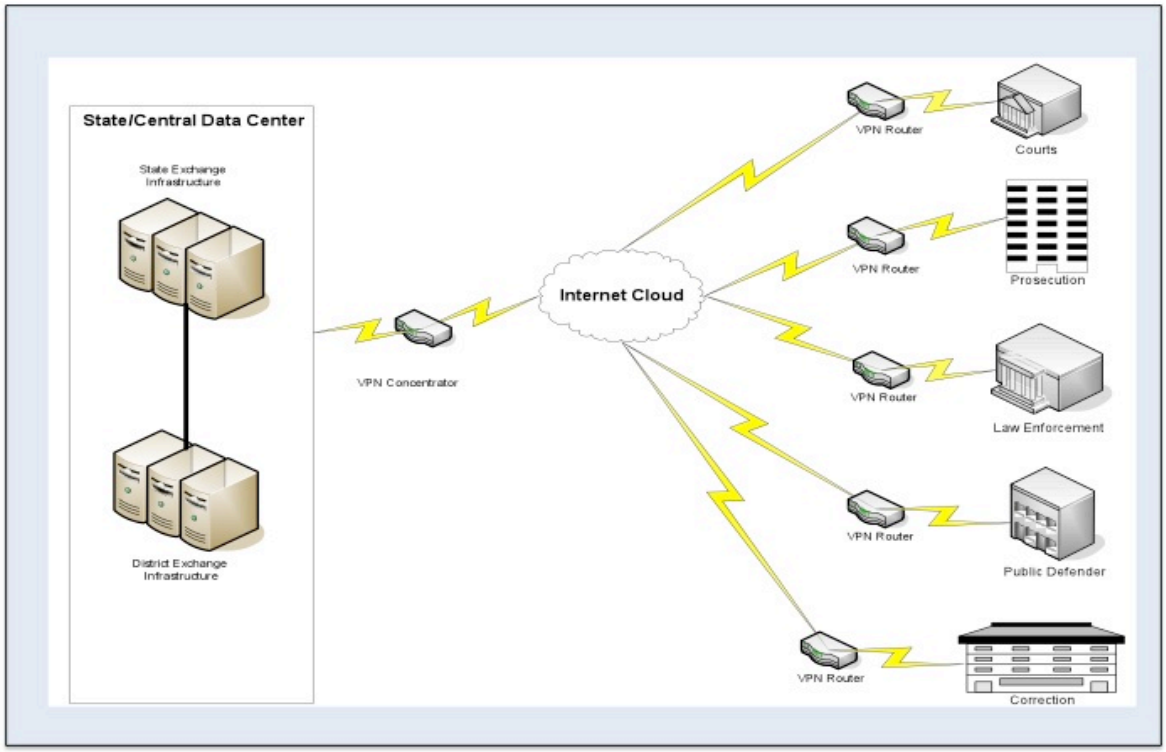
Phase I tactics are described below.

4.1.1 Deploy Basic Technology Infrastructure

GeorgiaJDX must deploy a basic technology backbone/foundation for the G-ISE architecture. Based on adopting an incremental approach, the infrastructure deployed in Phase I is robust but not expensive. As the G-ISE architecture expands to include more counties, circuits and districts, some open source components can be replaced with more robust (but also more costly) components. This approach allows the G-ISE architecture to prove its value with minimal investments and then grow as volume increases and as funding is identified.

Figure 8 graphically depicts the technology infrastructure recommended for Phase I. One server with three virtualized servers supports the district exchange infrastructure and one server with three virtualized servers supports the state exchange infrastructure. Virtualization software allows each physical server to be partitioned into multiple logical machines so numerous components can be supported on one server. In Phase I, the district server is partitioned to represent two districts. Each district server can be partitioned to support the components its district exchange infrastructure.

Figure 8: Phase I G-ISE Infrastructure



The specific hardware and software components required to assemble the Phase I infrastructure are detailed in Table 7. Specifications are provided as guidelines; the exact components may vary somewhat due to availability at the time of acquisition. Cost estimates are not provided as hardware and software prices change frequently as new models and versions are released . Specific costs for miscellaneous items such as power, cabling and cooling depend on the existing capabilities of the data center at which the components will be hosted. As depicted and described in earlier sections, the state exchange infrastructure and district exchange infrastructure physically reside at the state data center.

Table 7: Phase I Hardware and Software Requirements

Component Type	Specification	Qty	Phase I Requirement	Future Phase Requirement
CISCO VPN Concentrator	Cisco ASA 5520	1	Supports approximately 200 connections	May need to be replaced once more connections are established
Dell Rack Server	Dell Rack, Console, etc	1	Supports 4 to 5 physical machines	May need additional racks if additional units are acquired
Miscellaneous Cost	Cabling, Power Supply, Cooling, etc,	1	Depends on capabilities of hosting data center	Depends on capabilities of hosting data center
Tower/Rack Server – Virtualized Server	R 905, 4 Quad-Core processor with 64GB RAM, 8 x 146 GB Hard Drives	1	One server required for Phase I. Server has capacity to support up to 6 virtual servers.	1 to 2 additional servers anticipated to scale up over time
Virtualization Software	VMware vSphere 4.0 3-year subscription	1	3-year subscription with renewal after 3 years	For each additional machine, an addition copy of this software is required.
Virtualization Management	VMware vCenter 3-year subscription	1	3-year subscription with renewal after 3 years	Can be used across multiple physical machines
Windows 2008 OS	Windows 2008, 64bit	3	3 virtual machines configured in Phase I	1 additional license required for each additional virtual machine configured
Windows 2008 OS	Windows SQL Server, 64bit	1	One machine is a database server	1 additional license required for each additional database server configured
Message Bus	Jboss Stack, Support license	1	Open source software	Need to migrate to a more robust message bus with built in persistence Could potentially utilize state message bus
Certificate Server	Openssl		Open source software	Consider commercial products to replace the open source server

Component Type	Specification	Qty	Phase I Requirement	Future Phase Requirement
Tower/Rack Server – Virtualized Server	R 905, 4 Quad-Core processor with 64GB RAM, 8 x 146 GB Hard Drives	1	One server required for Phase I. Server has capacity to support up to 6 virtual servers.	1 to 2 additional servers anticipated to scale up over time
Virtualization Software	VMware vSphere 4.0 Advanced 3 year Subscription	1	3-year subscription with renewal after 3 years	For each additional machine, an addition copy of this software is required.
Virtualization Management	VMware vCenter 3-year subscription	1	3-year subscription with renewal after 3 years	Can be used across multiple physical machines
Windows 2008 OS	Windows 2008, 64bit	3	3 virtual machines configured in Phase I	1 additional license required for each additional virtual machine configured
Windows 2008 OS	Windows SQL Server, 64bit	1	One machine is a database server	1 additional license required for each additional database server configured
Message Bus	Jboss Stack, Support license	1	Open source software	Need to migrate to a more robust message bus with built in persistence Could potentially utilize state message bus
Certificate Server	Openssl		Open source software	Consider commercial products to replace the open source server
CISCO VPN Router	Cisco ASA 871	Per agency		

4.1.2 Develop and Deploy "Quick Wins"

A number of "quick wins" have been identified to be implemented to provide substantial value to the counties and circuits in the State of Georgia. These include exchanges (Information Exchange Package Documents) and Applications/Portals. Each addresses multiple criteria, including primary focus on identifiable public safety business drivers. The identified exchanges, as well as a shared application and a portal, can be developed and deployed in selected circuits to all participants to begin realizing value and benefit and to generate success stories to drive additional GeorgiaJDX participation. Each is described below.

Information Exchanges

Information exchanges and IEPDs are based on NIEM 2.0 standards and the NIEM exchange development methodology. These exchanges are developed once and implemented over time by all Information Sharing Community members. This exchange development approach is very cost-effective, as the GeorgiaJDX community, not any particular agency or vendor, owns the exchanges and makes them available for all members of the Information Sharing Community to implement. While numerous exchanges have been identified, prioritization based on business impact and the needs of the Information Sharing Community members is essential. As the NIEM-conforming information exchanges and IEPDs are developed, each can be implemented by county/circuit IT support and/or local system vendors depending on the needs and skills of the adopting agencies.

The following information exchanges are considered for development:

Intra-County

- Accusation
- Bonds (Notification & Release)
- Court Calendar Event
- Disposition
- Incident Report
- Indictment
- Notice of Appointment
- Order of Dismissal
- Warrants (Issued & Served)

Inter-County

- Accusations
- Bond Notification
- Bond Release
- Court Calendar Event
- Court Production Order
- Detainers
- Disposition

- Indictment
- Investigation
- Jail Drop Off Notification
- Notice of Appointment
- Order of Dismissal
- Warrant Served

County to State

- Court Production Order
- Sentencing Package
- Jail Drop Off Notification
- Bench Warrants
- Jail Census
- Jail Pick Up Request

Applications/Portals

Included in Phase I are an application and a portal that benefit all members of the GeorgiaJDX Information Sharing Community. Each is described below..

Sentencing Package – Counties currently forward sentencing packages to the Georgia Department of Corrections manually. This process is time-consuming and expensive as it delays transfer of financial responsibility from the county to the state of those sentenced to incarceration at Department of Corrections facilities. The Sentencing Package application enables counties to deliver the sentencing package to the Department of Corrections electronically upon completion of disposition, thus speeding the transfer of financial responsibility from counties to the state.

Offender Lookup Portal – The Offender Lookup Portal enables agencies to search and locate offenders and to generate census lists of offenders. This portal offers substantial benefits to the justice community as it enables agencies to identify if a person being sought is already in a local jail, thus enabling more efficient and cost-effective resource utilization

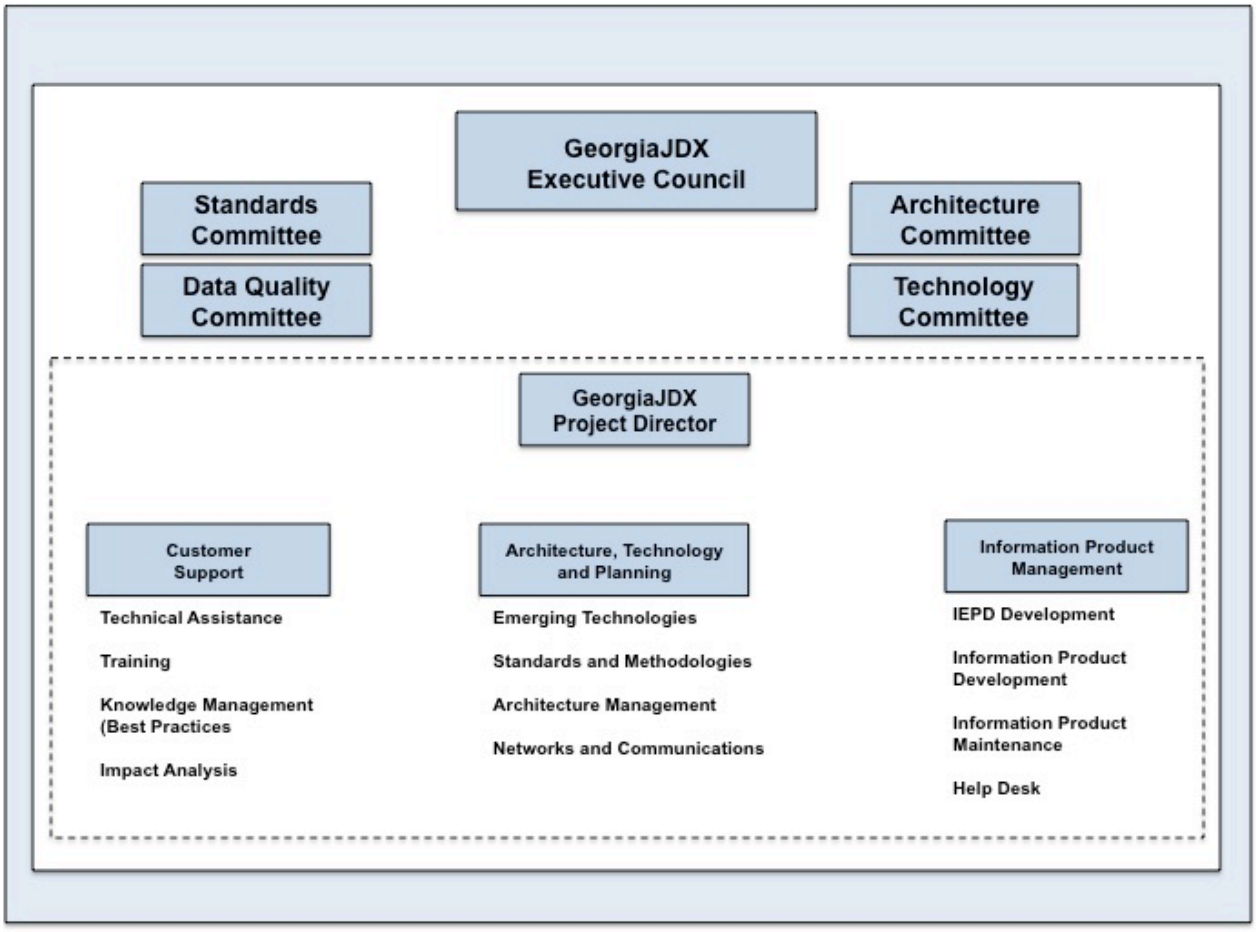
5 Governance Model

A strong governance model must be established for the GeorgiaJDX effort to be sustainable. As detailed in the NASCIO Enterprise Toolkit, sound architecture governance, which supports implementation and management of the enterprise architecture, is necessary to ensure the enterprise achieves its objectives. The Architecture Governance must be resilient enough to allow for those in primary governance roles to learn and adapt, manage risks, and appropriately recognize opportunities to take advantage of technology and act upon them.

Architecture Governance is the responsibility of executives, as well as stakeholders throughout the enterprise. Governance consists of the leadership, organizational structures, direction, and processes that ensure Information Technology (IT) sustains and extends the enterprise's mission, strategies and objectives in a planned manner. The purpose of Architecture Governance is to direct or guide initiatives, to ensure that performance aligns the enterprise business by taking advantage of the associated benefits, to enable the enterprise business by exploiting opportunities, to ensure IT resources are used responsibly and Technology Architecture-related risks are managed appropriately.

Figure 9 depicts the proposed governance model for the GeorgiaJDX project. This model is derived from the best practice models discussed by NASCIO and tailored to meet the needs of the GeorgiaJDX project. This model supports the architectural principles as well as the strategic direction of the GeorgiaJDX project, which states the local architecture at the agency level is managed and controlled by the agency. The shared information products are monitored and maintained by committees at the GeorgiaJDX level. This concept allows all counties to leverage their investment and create an Information Sharing Community that allows every agency to "do more with less". This approach allows the GeorgiaJDX project to provide a cost-effective and efficient mechanism for agencies across Georgia to share information.

Figure 9: GeorgiaJDX Governance Model



The GeorgiaJDX Executive Council provides the leadership and direction to the GeorgiaJDX effort. Four primary committees are specified, and additional working committees can be formed based on specific requests. The main objective of these committees is to review requests from the members and make recommendations to the Executive Council. A member of the GeorgiaJDX Executive Council heads each Committee. Once a recommendation is made to the Executive Council, the Council renders a decision and communicates the decision to the GeorgiaJDX Project Director. The roles of each Committee are described briefly below.

GeorgiaJDX Executive Council

The Executive Council provides the leadership and direction to the GeorgiaJDX project. It is comprised of stakeholders from each Circuit and provides policy and operational guidance to the project.

Standards Committee

The Standards Committee is responsible for establishing and monitoring the standards being utilized by the GeorgiaJDX project. This Committee reviews requests for changes from the members of the GeorgiaJDX project and makes recommendations to the Executive Council.

Data Quality Committee

The Data Quality Committee establishes data owners, creates data quality guidelines, creates data quality monitoring processes, monitors the data and identifies and resolves data quality issues.

Architecture Committee

The Architecture Committee establishes and monitors the enterprise architecture of the GeorgiaJDX project. This Committee periodically reviews the architecture to identify any modifications that may be required to stay abreast of emerging technologies or changes in business practices.

Technology Committee

The Technology Committee establishes and monitors the technology infrastructure for the GeorgiaJDX project. This Committee periodically reviews the technology infrastructure to identify any changes that may be required based on operational and policy issues.

Figure 9 also depicts a GeorgiaJDX support organization. This organization ensures the information sharing framework is supported and is led by the GeorgiaJDX Project Director. The Support Organization three divisions: Customer Support Division, Architecture, Technology and Planning Division and Information Product Management Division. The functions of each division are described below.

Customer Support Division

The Customer Support Division supports the needs of the members and stakeholder by providing the following services:

- Technical assistance
- Training, when requested
- Maintaining a knowledge management repository that identifies best practices and technologies being utilized in other courts and in other states.
- Conducting an impact analysis for every change requested by any of the members. This impact analysis is then presented to the Executive Council for a “go-no go” decision.
- Help Desk support

Architecture, Technology and Planning Division

The Architecture, Technology and Planning Division supports the strategic needs of the GeorgiaJDX project. This division performs the following functions:

- Reviews and comments on emerging technologies
- Maintains data standards
- Establishes data ownership
- Maintains standards for privacy and data security
- Maintains technology standards
- Establishes and maintains the enterprise architecture

Information Product Management Division

The Information Product Management Division supports the Information Products developed by the GeorgiaJDX project. This division provides the following functions:

- Develops and maintains information exchanges and IEPDs
- Develops and maintains information products
- Maintains the information sharing networks and infrastructure

- Establishes and maintains the G-ISE metadata repository that stores exchanges, services and other information product assets for use by members

6 Conclusion

This document defines and describes the Georgia Integrated Sharing Environment for the GeorgiaJDX community. Embodying public sector best practices and national data and architectural design standards, this G-ISE architecture provides a detailed strategy for achieving incremental, standard-based data exchange among GeorgiaJDX participants. The proposed governance model ensures a solid foundation for fair and effective management of the GeorgiaJDX initiative and the G-ISE architecture.