North Carolina
Government Business Intelligence
Competency Center
Program

June 2013

North Carolina
Office of the State Controller

David T. McCoy, State Controller

Table of Contents

Executive Summary 2

Business Intelligence 5

Government Data Analytics Center 6
I. Background 6
II. GBICC Activities 6
III. Budget 14
IV. Next steps 15

NC Financial Accountability and Compliance Technology Systems (NC FACTS) 16
I. Background 16
II. Data Sharing and Analytics Activity 17
III. Challenges 22
IV. Budget 26
I. Next steps 28

Criminal Justice Law Enforcement Automated Data Services (CJLEADS) 29
I. Background 29
II. CJLEADS Statewide Operations 30
III. Application Releases 31
IV. CJLEADS Database Upgrade 32
V. Future Application Enhancement 32
VI. CJLEADS Challenges 34
VII. Next Steps 36

Appendices 37

Executive Summary

Session Law 2012-142, HB 950, expanded the State's existing data integration and business intelligence initiatives by creating the OSC Government Business Intelligence Competency Center (GBICC) to manage the State's enterprise data integration and business analytics efforts. The GBICC manages enterprise program activities as well as analytics projects and systems including the North Carolina Financial Accountability and Compliance Technology System (NC FACTS) fraud, waste and improper payment detection project. The Criminal Justice Law Enforcement Automated Data Services (CJLEADS) criminal justice system is a separate program that organizationally reports to the State Controller through the GBICC. Proposed legislation for FY 2013-2015 would change the name of the program from the GBICC to the Government Data Analytics Center (GDAC).

Unlike the dated model where data is a by-product of IT operations, the vision for the GBICC is to transform existing data assets into an information utility for the State's policy and operational leaders for their use in determining program investment, managing resources, and improving financial programs, budgets, and results. Throughout the nation Chief Data Officers are being used to manage data assets. This allows those responsible for IT to focus on their areas of expertise, information technology, architecture and acquisition.

While technology plays a key role in effective data analytics, the successful development of a statewide initiative depends upon State stakeholders who must be engaged, demonstrating their belief that enterprise data analytics will provide a sufficient return on investment in either dollars saved or that outcomes achieved will outweigh the cost of such projects. Strong communications and the ability to manage change and make the initiative relevant to the stakeholders require significant effort to ensure the advantages of the program make clear "what's in it for them" to the agencies and end users.

Consistent with OSC's past data integration efforts which have been "scoped to success", the GBICC has had a targeted focus and incrementally expanding the scope of applications as expertise and capacity grows. Currently, the GBICC is deployed in three areas of analysis, development, and support:

- The GBICC development and implementation of program management and governance policy and procedure as well as two pilot areas of data analytic capabilities
- The North Carolina Financial Analysis and Compliance Technology System (NC FACTS) automated enterprise fraud, waste and improper payments detection project
- The Criminal Justice Law Enforcement Automated Data Services (CJLEADS) integrated criminal justice application

The GBICC
The GBICC is currently engaged with two areas of analytics:

- **Workers' Compensation Insurance Fraud and Employee Misclassification**
  In collaboration with the Joint Legislative Committee on Workers' Compensation Insurance Compliance and Fraud Prevention and Detection and the Employee Misclassification Taskforce, the GBICC and the North Carolina Industrial Commission (NCIC) are developing analytics focused on the areas of employee misclassification and workers' compensation insurance compliance. In March 2013, Phase 1 work started with defining project scope, developing business requirements, and identifying the data needed to detect businesses operating in the State of North Carolina but failing to meet the State's worker's compensation insurance requirements. Phase 1 has been providing assistance in identifying, monitoring, and resolving non-compliance cases. Subsequent phases of analytics will focus on the use of data from various enterprise sources to support employee misclassification and worker's compensation fraud. To ensure that there is a clear benefit to the State of this work, the impact of this effort will be measured and documented in subsequent reports.

- **State Health Plan of North Carolina (SHPNC)**
  The Department of State Treasurer, Information Technology Division, previously managed the SHPNC data and analytics repository using SAS software. The SHPNC analytics repository experienced technical challenges that impacted performance and ability to meet the SHPNC's analytics needs. Because the NC FACTS fraud analytics and the SHPNC program analytics require much of the same data, the GBICC, working with the SHPNC, completed the migration of the existing repository capabilities to the GBICC technical environment. As the SHPNC begins working with new and updated data extracts associated with new health plan contracts that take effect on July 1, 2013, the combined GBICC repository will eliminate redundant development of new data extracts as well as reducing the State's licensing and storage costs.

The GBICC continues work on key areas of program management to facilitate the use of the states through data sharing and analytics including:

- Establishing a registry of available data for use by all State organizations
- Establishing governance policies, procedures, and guidelines to broker data sharing agreements
- Establishing data and metadata standards based on national standards and industry best practices and determining how enterprise data model management and standards will be implemented
- Building consensus and agency "buy-in" for the emerging GBICC initiative to ensure that efforts are focused on appropriate priorities and adding value to the agencies
- Establishing working groups of business stakeholders

The Government Business Intelligence Competency Center section of this document provides more detailed information regarding the GBICC effort and next steps.

NC FACTS

NC FACTS continues to develop automated fraud, waste and improper payment detection capabilities. While data sharing and agency commitment continue to present significant challenges, NC FACTS has continued to make progress on gaining access to key data sources. The Department of Commerce, Division of Employment Security (DES) employer tax compliance and benefit payment analytics has been a priority area of effort. The NC FACTS team has worked closely with DES staff to review and verify the data analysis to ensure that analytic models are accurately interpreting data and generating results. To date, the NC FACTS team has delivered 425 alerts to the DES tax compliance unit and 830 alerts associated with DES unemployment insurance claims. DES, beginning to work with those initial results, found the first 12 alerts researched proved to be actionable cases with a potential impact to be approximately one and a half million dollars. NC FACTS is currently directing efforts at operationalizing the DES data, analytics and results delivery to allow DES to incorporate the NC FACTS results into their business processes and case management tool.

A data sharing agreement with the Department of State Treasurer (DST) - State Health Plan of North Carolina has been executed and health plan member eligibility and claim data analysis has begun. The NC FACTS team is working with SHPNC to identify data and business requirements to perform health plan fraud analysis.

A data sharing agreement was recently executed in June 2013 with DST - Retirement System. Project activities to address retirement plan fraud and general program analytics will be implemented.

The NC Financial Accountability and Compliance Technology System (NC FACTS) section of this document provides detailed information about its development activities.

CJLEADS

CJLEADS operates as an independent section in the OSC and continues application support and enhancement activities to provide criminal justice professionals with access to comprehensive offender information. More than 26,500 users are trained and using CJLEADS statewide. The latest release of CJLEADS provided the ability to verify outstanding warrants against the Statewide Warrant Repository on a real-time basis.

The Criminal Justice Law Enforcement Automated Data Services (CJLEADS) section of this document provides detailed information about CJLEADS application support and enhancement activity.

Business Intelligence

Business data is a valuable resource for organizations in government and the private sector. Data enables organizations to analyze historical behavior, predict future trends and make decisions based on business facts rather than intuition and supposition. Over the years, however, data was managed by Information Technology offices and was gathered and stored in siloed data systems that were built to meet the business needs of individual organizations. When data is stored in varying formats and technical platforms, the process of gathering information from different lines of business can be complicated, time consuming, expensive and difficult.

Business Intelligence (BI) is a process that allows an organization to gather, analyze and report key information to improve business outcomes. BI focuses not only on the business process, but also on integral components that impact the business process including customers, employees, and key business stakeholders. Integrated, useful and accessible data about these key elements help an organization make effective, efficient and informed business decisions. With BI, the possible uses of data depend upon the business need, and analysis may be fluid as business users see their data and its value in new ways. As a result, unlike most information technology projects, BI projects rarely follow the standard systems development lifecycle.

Historically, operational information systems developed by focusing on automating processes, reducing costs and improving performance. With typical systems, a business need is identified, scope and business requirements are outlined, and cost and timelines are established. The project moves through the systems development lifecycle of design, build and deploy, with the goal to complete the project on time, under budget and in accordance with the scope.

Chief Data Officers, on the other hand, recognize that data analytics and business intelligence projects are built on the premise that there is meaningful information to be found in the data collected in an organization's operational systems. Analytics projects cannot be managed with the same mindset of pre-defined outcomes, required tasks and detailed project plans to reach deployment. Instead, analytics projects strive to understand what business questions exist and how data might be used to answer those questions. Data analysts identify where data is available and where it is not available, how it can be matched to other data, aggregated, summarized and evaluated, and whether or not it is able to add value to the decision making process. As business users evaluate the information and resulting analysis, new questions, new directions, and new strategies are identified and the process repeats itself to refine the answers to the new questions.

Utilization of analytics means that projects will not fit the standard "IT" model for budgeting, contracts, project management reporting and benefits analysis. The benefit of data analytics projects may range from better informed decision making to more efficient and effective business processes to actual dollar savings resulting from better control, detection and prevention of fraudulent or improper payments. The GBICC is focused on providing quality enterprise analytics to support the State's business needs.

Government Business Intelligence Competency Center

I. Background

The Government Business Intelligence Competency Center (GBICC), established in Session Law 2012-142, HB 950, expanded the State's existing data integration and business intelligence initiative and provided statutory language promoting greater data sharing for statewide enterprise initiatives. The GBICC seeks to identify data integration and business intelligence opportunities that will generate greater efficiencies in and improved service delivery by State agencies. This effort includes all State agencies, departments, and institutions in the three branches of government.

To obtain further information about BI, the GBICC vision and program requirements, please see the February 2013 North Carolina Government Business Intelligence Competency Center Program Report located at http://www.osc.nc.gov/GBICC/GBICC_Feb_2013_Legislative_Report.pdf

II. GBICC Activities

GBICC Project Management Activities

Worker's Compensation Fraud and Employee Misclassification Detection

Worker's compensation fraud and employee misclassification are closely related and both result in exposure to the State, its economic and business environment, and its workforce. Risk to employees increases when businesses fail to properly report their employees and provide workers' compensation coverage. An employee injured in a work-related accident may find that they are not properly covered and incur unexpected medical expenses and lost wages. When these workers have no insurance coverage and no means to pay, the State incurs the costs of medical treatment and social services. The failure of some businesses to properly report their employees and pay for workers' compensation coverage results in a competitive advantage over businesses that comply with State law (and build the cost of coverage into the cost of their products and services). Conversely, when employees inappropriately or fraudulently receive a worker's compensation benefit, the employer and insurance companies bear the cost of the fraudulent expenses.

In January 2013, both Joint Legislative Committee on Worker's Compensation Insurance Coverage Compliance and Fraud Prevention and Detection and the Employee Misclassification Taskforce, recommended that the NCIC work with the GBICC to develop workers' compensation fraud and employee misclassification analytics.

The GBICC and the NCIC signed a data access and usage agreement in March 2013 and held meetings to develop preliminary scope of work and identify short and long-term priorities. Phase I of the effort is focusing on identifying businesses operating in the State

of North Carolina but failing to carry required workers' compensation insurance. Using data from the NCIC and key partner agencies, the analytic is identifying active businesses, matching them with worker's compensation insurance coverage data, and providing alerts to NCIC staff of companies that appear to lack appropriate coverage. In addition, the analytic searches for policy gaps in coverage, failure to renew coverage, and unexpected cancellations of coverage. Initial alerts based only on NCIC data have been related to gaps in coverage and have provided actionable leads for NCIC staff investigation purposes.

The GBICC is working with NCIC to operationalize the workers' compensation compliance alerts, monitoring and communication processes and subsequent case management tool integration.

The results of these efforts will be measured and reported in subsequent reports. A baseline non-compliance level is being established to determine the impact of this first major effort to bring businesses back into compliance. When this is complete, NCIC will establish a process to monitor compliance levels on an ongoing basis to ensure that their enforcement initiative is working effectively. Additional metrics will also be established to determine the impact on the insurance industry through improved participation and compliance as will metrics to estimate the impact on the State through reduced public assistance support, due to enhance coverage.

Phase II priorities will focus on expanding analytics to evaluate employee misclassification and workers' compensation fraud.

The GBICC and NCIC are currently working with Department of Commerce, Division of Employment Security (DES) to finalize a data access and usage agreement to allow the use of DES data to identify active businesses for comparison against workers' compensation coverage data. Other key sources of information may include:

- The Department of Justice
- The Department of Insurance
- The Department of Labor
- The Department of Revenue
- The Department of Secretary of State

State Health Plan Analytics Repository

The North Carolina State Health Plan for Teachers and State Employees (SHPNC) relies on data warehousing to support their business operations. Currently, third-party vendors manage membership and claims processing. SHPNC receives monthly extracts from the third parties to support reporting and analytics. The Department of State Treasurer, Information Technology Division, managed the SHPNC data and analytics repository using SAS software to support program metrics analysis and reporting and was

experiencing technical challenges that impacted performance and the ability to meet the SHPNC's analytics needs.

SHPNC is currently working with NC FACTS to establish fraud analytics related to member eligibility and claims processing. Because NC FACTS fraud analytics and the SHPNC program analytics require much of the same data, this enabled the move of the SHPNC analytics repository to the GBICC technical environment, reducing licensing and storage costs and gaining processing efficiencies.

The GBICC and SHPNC migration of the SHPNC analytics repository into the GBICC environment resolves current technical issues. The common repository, used by both GBICC and NC FACTS, allows the State to perform data integration and analysis work once to support both analytic needs.

The SHPNC analytics repository migration was completed in May 2013 and accepted by the State Health Plan. The GBICC will continue to work with SHPNC on data extract modifications related to new vendors associated with the SHPNC's contract changes on July 1, 2013.

Department of State Treasurer

As the DST, Retirement Division began work with NC FACTS on retirement fraud, waste and improper payment detection analytics, the Retirement Division recognized the value of leveraging the data in the repository to other Retirement Division analytics as well. The GBICC will continue to work closely with the NC FACTS and Retirement Division teams to support general retirement program analytics as well as possible Unclaimed Property analysis.

Division of Employment Security

As the Division of Employment Security progresses through its unemployment insurance fraud analysis, they have also recognized the value of additional program analytics. The GBICC is working closely with the NC FACTS and DES teams to identify key program metrics and analysis needs as well as executive-level reporting for DES management.

Education and Workforce Data

Existing (and proposed) legislation direct the GBICC to coordinate individual-level student data and workforce data from all levels of education and the State workforce. The GBICC program resources have researched the P20W Longitudinal Study as well as the Common Follow-up Program to understand the State's current efforts in these business areas. Educational programs and valid objective results, whether related to vocational training, industry-specific training, university level programs, or a community's K-12 options, are all important factors in strengthening the economy of the State. This information may assist state and local economic development programs by providing reliable information about educational programs that demonstrate the strength of specific

institutions that support prospective company interests. Education information can also assist local educational agencies and regional programs in working to improve specific programs to provide greater parity among the State's educational programs and offer opportunities to optimize resources among the various entities. The State Controller has designated the GBICC Program Manager to act as his designee on the North Carolina Longitudinal Data Systems Board. The GBICC staff continues to work collaboratively with these programs to support the existing education community's analytics needs and to be able to share enterprise data sources to benefit the State.

Program Security and Data Integrity

The State's data provide a rich repository of key information to enable strategic and operational decision making. North Carolina citizens, however, have an expectation of privacy and a right to know that their personal information is protected. The GBICC protects the State's data in several ways:

- The GBICC repository, hosted by SAS, leverages a variety of stringent security measures including physical security related to the data center, virtual security to control access to the technical environment, monitoring and intrusion detection, penetration testing to identify and resolve system vulnerabilities, and personnel security through criminal background checks and security based training.
- The GBICC establishes Data Access and Use agreements with each data source owner agency to identify sensitive data, specify how that data can be used and for what purposes, and define appropriate security requirements for access. These agreements provide the requirements for key security components of the repository and user interfaces.
- The GBICC repository and applications provide data to meet specific business needs. Users cannot randomly search or "data mine" information from the repository. Access to data is limited to specific analytic models, filters, alerts and reports as defined by the data source agencies.
- The GBICC applications have full auditing capabilities to allow for reporting on data access by users of the GBICC systems.
- The GBICC applications are designed to use the North Carolina Identity (NCID) management application to allow users to authenticate to all GBICC solutions using their existing state-issued user identification and password.
- The GBICC applications leverage role based security, managing access to specific analytic capabilities and data sources in accordance with data access and use agreements associated with each business area.

Enterprise Reporting Environment

While working with data to conduct fraud analytics, the NC FACTS and partner agency teams have recognized that data integrated and evaluated for fraud provides a valuable repository for other potential agency program analytics. The single GBICC repository provides a mechanism to reduce duplicative data integration design and development work, data storage and repetitive maintenance and support. For example, after the State

Health Plan's data is incorporated into the NC FACTS repository for fraud analytics, the same data, coupled with other data available within the enterprise repository, will provide valuable information for other State Health Plan analytics.

The enterprise repository allows the GBICC to extract, transform and load the data once, then use the data for multiple purposes. The enterprise repository provides a shared environment with common security, user access, improved usability and consistent look and feel. A shared repository also allows for shared business services including training, help desk support and user administration.

While there are benefits of a shared repository, the enterprise nature of the repository will create additional complexity in the areas governance, security and cost allocation.

For a list of all data sources currently integrated into the enterprise repository, see Appendix B.

GBICC Program Management Activities

One of the most significant challenges with establishing the enterprise GBICC program is raising the awareness of the program throughout State government and implementing program policies that manage financial resources, project prioritization and operations.

Leveraging lessons learned in the initial pilot areas, the plan will provide detailed information of the program's requirements, objectives, and impact of the program's implementation and value to the State. With permanent funding for full time program personnel and funding to support the analytics software and hosting, the GBICC could significantly ramp-up efforts to build support and encourage adoption by State agencies critical to the long-term success of the program. As noted in the description of the two current projects (Workers' Compensation and the State Health Plan Analytics repository), the GBICC program resources will develop a business case to ensure each business intelligence initiative meets the enterprise program objectives and demonstrates benefits, in terms of program metrics, process efficiencies and/or cost savings, to justify the cost to design, develop and support the associated analytics.

Program management activities will include:

- Definition of a GBICC Mission Statement and Key Objectives

  The GBICC is a program activity that brings value to the State through efficient, effective data sharing and business intelligence efforts. The purpose of the initiative is to support the effective and efficient development of State agency business intelligence capability in a coordinated manner and reduce unnecessary information silos and technological barriers. The initiative is not intended to replace transactional systems, but is instead intended to leverage the data from those systems for enterprise-level State business intelligence. As the GBICC matures, demonstrates positive results, and brings value to State business users, the vision is to create a

program where business owners seek guidance and support from the GBICC for enterprise analytic efforts.

To clearly define an action plan providing program requirements, objectives and end-state of the GBICC, the purpose of the GBICC must be understood by stakeholder agencies and organizations. The GBICC has met with key individuals and groups including state agency CIOs to ensure that the GBICC program is established with guiding principles focused on facilitating business intelligence that assists the State's agencies and workforce.

Short-term objectives include:

- Defining the GBICC Mission Statement and Key Objectives
- Updating web content and expanding awareness of the GBICC
- Establishing policy and procedures for governance and data standards
- Initiating pilot business intelligence efforts

Long-term objectives include:

- Establishing governance support to include analytics end-user communities and advisory groups
- Institutionalizing governance and data standard policies and procedures
- Identifying sustainable program resources and funding
- Identifying future business intelligence areas of focus

- Establishment of Program Standards, Policies and Procedures

Achieving efficiencies in developing BI and ensuring that solutions meet the business needs requires program level standardization. GBICC resources will use research results to develop program policy, procedures and best practices. Areas of focus for program management include:

- Clear and consistent messaging about the GBICC mission and objectives

  To ensure the long-term success of the GBICC program, agency and organization stakeholders must clearly understand the purpose of the GBICC and how the GBICC can support their business needs. This will require ongoing communication and input from stakeholder agencies to frame the creation of the GBICC and establish priorities. The GBICC will continue to hold one-on-one meetings with senior leadership to ensure that agencies are aware of the GBICC mission and objectives. In addition, GBICC personnel are currently developing web content to provide information to stakeholder organizations. Additional efforts will be directed at establishing key advisory groups and end-user communities to provide input and feedback on GBICC program efforts.

- Data Inventory and Standards

  Data inventory, standards, and management are critical to the ability to provide quick, agile, and consistent data content to meet dynamic business needs. Research on industry standards and approaches to the concepts of data inventory, master data management, and data standardization is ongoing. Once defined for the GBICC, these will ensure that data integrated into the GBICC analytics repository provides reliable, timely information in clearly defined formats enabling stakeholders to analyze and interpret the data with common understanding. A challenge with establishing data standards is that legacy, stand-alone systems store data in a variety of methods and standards that vary widely across these applications. While the GBICC can set standards for data integrated into the enterprise repository, it would be overly time consuming and costly to retrofit legacy systems to new data standards. As new systems are proposed, however, these standards can guide the State's development toward enterprise data consistency.

  The State Controller has proposed the creation of a State Data Office, to work in concert with the GBICC, to set data standards, ensure quality control, facilitate the interaction of cross-department discussion to enable sharing of data and oversee the strategic business application of the State information assets enterprise-wide.

- Governance

  The GBICC is working to include a privacy framework for BI that provides adequate access controls and end-user security requirements. Governance policies and procedures provide clear instructions on the protection of confidential information protected by federal or State rules and regulations and defines the use of the data and determines requirements for auditing, backup and recovery and other controls. Leveraging lessons learned from CJLEADS and NC FACTS, the GBICC is defining governance documents and protocols for data security and privacy. Governance for data security will include among other things:
  - Physical security controlling physical access to technical infrastructure and data centers
  - Virtual security controlling remote access to information in the GBICC technical environment
  - Encryption/transmission security to protect data in transit and storage
  - Backup and retention to prevent data loss or corruption
  - User authentication using NCID
  - Role-based security to control access to specific data tables or fields
  - Auditing capabilities to track and monitor access to and usage of GBICC data
  - Penetration testing to assess and resolve any technical infrastructure or application vulnerabilities
  - Intrusion detection/unauthorized access monitoring to detect and stop any malicious or abnormal activities

- Service level agreements to ensure technical environment and application meets business operations requirements
- Personnel background check and certifications as needed

Governance is also required to ensure that business intelligence efforts throughout the State meet the State's established standards. Governance related to program management will include:

- Guidelines and procedures for collaboration work and oversight of business intelligence efforts throughout the State
- Project prioritization guidelines to determine the most effective allocation of GBICC resources
- Standardized methods to develop business case justification, cost/benefit analysis and program metrics to ensure State resources are most effectively utilized as well as on-going impact assessments
- Regular oversight and review of State licensing and BI capabilities to reduce redundancy, ensure consistency in standards and technology and to achieve economies of scale

- Refinement of the Technical Infrastructure and Analytics Capabilities

The ability to support enterprise analytics requires quick, reliable and accurate access to data in a standard, consistent format. Enterprise efficiencies begin to be achieved when data, integrated, cleansed and analyzed for one business purpose, is available to provide more robust information for other purposes. Throughout the State today, agencies are sharing information, and the lack of an enterprise repository results in multiple agencies expending resources to extract, analyze and store multiple copies of the same information to support business needs.

As anticipated, the data integrated to support criminal justice and fraud, waste and overpayment through the data integration programs established a foundation of information for a wide variety of analytics. Because of this, OSC negotiated with SAS to combine these project technical infrastructures to support all GBICC program efforts. As a result, the GBICC will work with SAS to refine enterprise technical architecture to support all GBICC initiatives. Enterprise architecture provides the ability to:

- Reduce redundant extract, transmission, cleansing and storage of data needed for agency analytics
- Define and manage the security and control of data in a single environment
- Define and manage end-user access through a consistent user administration process
- Ensure that all technical support personnel with access to data are consistently vetted and authorized for project work
- Audit all access to and usage of data across the enterprise business intelligence capabilities

- Project Reporting

  Business intelligence and data analytics is a unique combination of applying known business rules and knowledge as well as performing creative "what if" analysis to understand how data can support business decisions. Business intelligence projects do not follow normal project management processes. Business intelligence is often an iterative, sometimes trial and error approach to understanding the data and how it can support dynamic changing business needs.

  The GBICC will continue to work closely with the State Chief Information Officer and the State Enterprise Project Management Office to consider alternative approaches to reporting GBICC project definitions, schedules, resources and cost/benefit analysis.

III. Budget

Session Law 2012-142, HB 950 appropriated $5 million in non-recurring funds to support the enterprise BI program. Of that amount, the OSC may use $750,000 for the administration of the program. The remaining funds are reserved for initiatives recommended to and approved by the General Assembly.

The GBICC executed a contract with SAS to initiate business intelligence projects under the GBICC program. The contract provides analytics service resources and will leverage the NC FACTS technical infrastructure. The GBICC contract provides analytics licensing and services through December, 2013. The following chart shows the expenditures as of May 31, 2012.

Estimated FY 2013 as of May 31, 2013	**FY 2012-2013 Budget**	**Available Balance**
GBICC Funding		
Program Initiatives	$4,250,000	
Program Administration	$750,000	
	$5,000,000	
GBICC Expenditures		
Total Project FY 2012-2013		
State Project Team Expenditures	$1,033,796	
GBICC Total	**$1,033,796**	**$3,966,204**

The OSC must hire additional full-time staff to support the on-going GBICC efforts. Recurring funding is necessary to establish permanent positions for the skilled program

resources needed to support enterprise BI efforts. In addition, funding to support the analytics licensing and development services will be required to sustain the GBICC program efforts.

IV. Next steps

The GBICC will continue the implementation of key GBICC Program Management components to enable the development of the GBICC Plan of Action. Top priorities for GBICC program management include:

1. Building consensus and agency "buy-in" for the emerging GBICC initiative to ensure that efforts are focused on appropriate priorities and adding value to the agencies. The ability to build consensus will depend on developing a clear concept of the GBICC and how it will bring value to the agencies.
2. Establishing working groups of business stakeholders to assist with business needs assessment and project prioritization and user community members to provide feedback on analysis needs, techniques and tools.
3. Establishing a register of available data – using the inventory responses, the GBICC will identify a process to register data sources and data source owners for use by all State organizations.
4. Establishing governance policy, procedures, and guidelines to broker data sharing agreements across organizations including the creation of a legal advisory group of state and federal privacy, disclosure and security regulations subject matter experts who can provide guidance on data sharing issues and agreements
5. Establishing data and metadata standards based on national standards and industry best practices and determine how enterprise data model management and standards will be implemented
6. Other program areas for consideration include:
    a. Contract and license management.
    b. Support/Help desk.
    c. Technology, architecture and infrastructure.
    d. Production system management.
    e. Training and Change Management – enhancements, upgrades, and scope expansion.
    f. Consulting to business units.

The GBICC's project activities for analytic focus include:

1. Workers compensation fraud analysis and employee misclassification
2. North Carolina State Health Plan analytics repository migration to the GBICC
3. Division of Employment Security program analytics
4. Department of State Treasurer Retirement Division and Unclaimed Property analysis

In addition, the GBICC will continue to evaluate the inventory results and work with State agencies to identify business needs and priorities for future development efforts.

NC Financial Accountability and Compliance Technology Systems (NC FACTS)

I. Background

Session Law 2011-145, HB 200, directed the Office of the State Controller (OSC) to develop an enterprise process to detect fraud, waste and improper payments throughout state government. Session Law 2012-142, HB 950 placed the North Carolina Financial Accountability and Compliance Technology System (NC FACTS) program under the Government Business Intelligence Competency Center (GBICC) to ensure coordination and efficiencies in the development of the State's business analytics capability.

To develop an enterprise program to detect fraud, waste, and improper payments across state government, OSC is partnering with state agencies to identify business needs in the area of fraud, waste and improper payment analysis, detection, and reporting. Data integrated to support one agency's business needs will likely add value to fraud analysis for other agencies and the state government enterprise. Agency partnerships, with associated data governance agreements that define the data to be shared, technical and user access security protocols, auditing requirements, and more, are critical to North Carolina's enterprise business intelligence efforts.

OSC entered into a two-year contract with SAS, with a maximum cost of $8 million to develop NC FACTS. The contract defines a public-private partnership with the State's data integration vendor contributing resources in the amount of $5 million in each of the two contract years (FY11-12 and FY12-13). This partnership ensures active participation and commitment from the State and the data integration vendor and focuses on providing a strong return on the State's investment. The parties will coordinate efforts to report benefits realized for each area of fraud, waste or improper payment analysis.

NC FACTS applies advanced analytics to the State's integrated data to create alerts about suspected fraudulent, wasteful, or improper payment activity. Using key identifying and demographic information, NC FACTS is able to develop relationships and linkages among multiple data sources to indicate potential collusion and/or criminal activity. Because confidential data is critical to the ability to perform fraud analysis, NC FACTS is implementing the appropriate technical architecture, security, and user access parameters to protect data in accordance with federal and state regulations.

While the program will expend considerable effort on data collection and integration, support for the business programs responsible for analyzing and investigating the identified fraud incidents is critical. This effort, in collaboration with the business area, will identify the business processes and resources required to recover fraudulent or improper payments, to prevent future incidents of fraud, waste and improper payments, and to ensure that the analytics used to identify these incidents are continually being improved and refined to more accurately evaluate risk and fraud patterns.

NC FACTS has made significant progress in some business areas, but the team continues to expend considerable resource time in gaining agency stakeholder commitment and access to data. The project team has focused on developing data sharing best practices, addressing inhibitors to data sharing and understanding agency operational priorities and resources that often limit the agency resources committing to assist NC FACTS. Agencies, accustomed to managing data within their applications, struggle with balancing their duty to protect the privacy of "their" data with the need to share data to ensure that tax dollars are appropriately used to provide the best value and services for the citizens of North Carolina.

II. Data Sharing and Analytics Activity

The development of risk analysis and fraud detection at the enterprise level is a significant undertaking and an iterative process. Agencies participating in the program may realize "quick hits" based on verification of known business rules within the first few months of sharing these data. Development of mature analysis, however, will evolve over time as North Carolina's integrated data is used in developing more sophisticated analytic and predictive models, filters, and network analysis. These analytic tools will be further refined based upon analysis, verification and feedback on the fraud alerts generated by the system.

For more information about the program approach to analytics development, the technical infrastructure and the governance model, please see the February 2013 North Carolina Government Business Intelligence Competency Center Program Report located at http://www.osc.nc.gov/GBICC/GBICC_Feb_2013_Legislative_Report.pdf

The Department of Commerce - Division of Employment Security

In early October, 2012, the Division of Employment Security (DES) began transmission of critical data related to the State's unemployment insurance program.

Analytic efforts for Division of Employment Security are focused on two different business areas. The first, employer wage and tax reporting, identifies where suspect information and/or activity that may indicate fraudulent or improper representation of employees, wages, and associated unemployment taxes as well as potential fictitious businesses established either for the purposes of avoiding UI tax payments or fraudulent collection of UI benefits. The second area of analysis focuses on benefit eligibility and payment information to identify fraudulent or improper UI benefit payments.

NC FACTS has delivered 425 alerts to the DES tax compliance unit. These alerts identify business behaviors which may indicate possible fraud or non-compliance. Alerts in this area included:

- Undocumented succession where a business owner establishes a new business with a lower unemployment tax rate and move employees to the new business, avoiding a higher taxable rate.

- Fictitious businesses where a company registers with DES, files retroactive wage reports, and has a significant number of employees' filing claims and drawing benefits at a rate faster than the accumulated taxes are paid. Using other data in the enterprise repository, data analysis often reveals other suspect characteristics such as unlikely physical addresses, unemployment claimants sharing the same address and claimants with no history of receiving other services from the State (e.g. no DMV records).

DES is investigating the employer related alerts that have been delivered and have indicated that the first 12 alerts proved to be actionable cases with a potential impact to be approximately one and a half million dollars.

The investigation of unemployment claimants and eligibility has identified over 830 alerts associated with DES unemployment insurance claims. These initial alerts generated situations where:

- Unemployment claimants who received benefits after date of death. Although DES verifies deceased data at time of payment, NC FACTS was able to identify those claimants whose deceased records were updated after the unemployment payment and alerted DES to block future benefits.
- Unemployment claimants who were incarcerated in prison during the time they received benefits.
- Unemployment claimants who were in custody in jail during the time they received benefits.
- Unemployment claimants who were receiving payments from the State's BEACON payroll system during the time they received unemployment benefits.
- Unemployment claimants appeared as being employed and paid by a business on a quarterly wage report during the time they received unemployment benefits.

DES is investigating the claimant related alerts. The business process to investigate these alerts takes time and often requires information from the employer and claimant interviews to determine if fraud or overpayment has occurred. At this time, DES has not provided an estimated potential savings from the analysis, but has indicated that the ability to prioritize the alerts will assist them in optimizing resources for investigations, stop future payments, and support recovery efforts.

While DES continues to review and take action on the alerts delivered to date, NC FACTS is working with SAS to operationalize the analytics process and application user interface. The operationalization process includes establishing the following:

- Production ETL and Analytics - building production level processes to extract, transform and load data, then match that data with other enterprise data sources and apply analytics through known business rules, statistic and pattern analysis, predictive analysis and relationship or linkage analysis.
- User Interface – customizing SAS analytics tools including the SAS Fraud Framework to provide a user friendly tool that allows DES to review, assign and disposition fraud alerts and track those alerts through investigation and resolution.

- Security – developing the required user authentication and role based security to ensure control over data access
- Business Operations – developing the supporting procedures for the DES fraud application including training, auditing, Help Desk support and user administration

As the initial areas of analysis are operationalized, the NC FACTS team will work with DES to implement real-time validation based on the "quick hit" analysis. For example, if real-time access to data can detect that an individual requesting unemployment insurance benefits is currently in jail or prison, DES may be able to stop a payment rather than having to attempt to recoup the funds at a later date.

The Department of State Treasurer – State Health Plan of North Carolina

The SHPNC mission is to provide quality health care products and services for the health and well-being of their members while ensuring fiscal responsibility and transparency. NC FACTS tools will support the SHPNC and its ability to identify suspicious activity associated with provider billing and member benefits.

In September, 2012, the SHPNC signed a Data Access and Usage Agreement (DAUA) to allow NC FACTS to receive and analyze health plan data. The NC FACTS team has worked with the SHPNC to identify the necessary data files and elements and requests are being submitted to the SHPNC vendor partners to develop data extracts. NC FACTS will implement the standard health care scenarios available within the SAS Fraud Framework. The first analysis will support a review of professional, hospital and drug claims in an effort to identify providers and members whose services seem to fall outside of the range of their peers. Since SHPNC has an existing contract with their vendors to perform fraud analysis, it is expected that the NC FACTS analysis will focus on areas of fraud where the vendors may not have had previous insight.

As noted in the GBICC section of this report, the SHPNC currently leverages a SAS analytics reporting repository. Recognizing that the NC FACTS program and the SHPNC program analytics require many of the same data feeds, it was determined that integrating the SHPNC analytics repository into the GBICC environment will allow the State to reduce licenses and avoid duplicate data storage and technical infrastructure and support costs.

Department of State Treasurer - Division of Retirement

The Department of the State Treasurer (DST) administers the Teachers and State Employees and Local Governments pension plans for North Carolina's 850,000 public employees and retirees. The Department of State Treasurer executed a data access and use agreement in May 2013. Scope discussions and business requirement definitions are in the process of being scheduled.

P-card Analysis

During evaluation of North Carolina Accounting System (NCAS) data, the NC FACTS team began analysis of procurement card data (P-card). By incorporating Bank of America transaction detail, and BEACON employee status, the analysis provided insight into P-cards activity and a verification of authorized agency users. While data analysis did not identify areas of suspected fraud, it did provide integrated reports that could benefit agencies in verifying of unusual activity and improving internal controls. The Office of the State Controller, Risk Mitigation Section, reviewed P-cards from an internal control perspective and documented requirements for P-card reporting which will assist agencies by reducing manual review and improving internal control and adherence to State procurement and cash management policies and procedures.

The GBICC program will initiate meetings with Department of Administration procurement to determine next steps to operationalize the use of these reports in P-card management.

Department of Transportation – Division of Motor Vehicles

The Division of Motor Vehicles maintains vehicle registrations and driver license data for North Carolina citizens. This information has been identified as data which can be utilized to support analytical model development associated with various business areas.

The DMV agreed to participate in the NC FACTS program. A DAUA has been executed to provide access to the DMV data. While the data extract will currently provide only partial Social Security Numbers, the data will still provide key information to support enterprise data analytics.

Future Analytics

Data Sharing to Locate Absconders

While conducting analysis for fraud, waste and improper payments, the NC FACTS and partner agencies are identifying additional ways to support key business needs using data that has been integrated to support the fraud analysis. Session Law 2012-170, H.B. 1173, states that the, *"court may order the suspension of any public assistance benefits that are being received by a probationer for whom the court has issued an order for arrest for violation of the conditions of probation but who is absconding or otherwise willfully avoiding arrest. The suspension of benefits shall continue until such time as the probationer surrenders to or is otherwise brought under the jurisdiction of the court. For purposes of this section, the term "public assistance benefits" includes unemployment benefits, Medicaid or other medical assistance benefits, Work First Family Assistance, food and nutrition benefits, any other programs of public assistance under Article 2 of Chapter 108A of the General Statutes, and any other financial assistance of any kind being paid to the probationer from State or federal funds."*

The DES unemployment insurance analysis compared benefit payments with individuals who were incarcerated during the period of benefits, NC FACTS also found individuals who were receiving unemployment benefits and were identified in CJLEADS as absconders. Incorporating other public assistance benefit data, along with the unemployment insurance information in the GBICC/NC FACTS environment, may assist the courts in identifying individuals absconding from supervised probation for whom public assistance benefits can be suspended. In addition, the ability to identify absconders, and their associated public assistance benefits, may offer the opportunity for key stakeholder agencies to work collaboratively to re-establish contact with individuals who are violating the terms of their probation.

While the NC FACTS team works with data source agencies to verify the accuracy of these initial data matches of absconders and unemployment insurance payments, the team will also initiate discussions with the courts and other social service organizations to understand how this data analysis may be able to support the efforts associated with Session Law 2012-170, H.B. 1173.

The Department of Health and Human Services

The Department of Health and Human Services (DHHS) provides some form of services for one out of every six North Carolinians. With an annual operating budget of $14 billion to meet these needs, the potential for fraudulent or erroneous payments exists. Recognizing the possibility for fraudulent activity to occur, DHHS has instituted many initiatives and investigative programs.

During interagency discussions related to DHHS anti-fraud efforts, DHHS, OSC, and SAS recognized considerable synergies between the current DHHS eligibility program and the NC FACTS initiative. With similar data needs, software licensing and hosting requirements, working collaboratively on these two projects offers the State the opportunity to cut costs while achieving common goals. DHHS, OSC and SAS continue to discuss tasks and timelines to merge these efforts.

In addition, OSC continues to work with DHHS to gain access to key sources of data, including vital records and eligibility data, and to identify areas of focus within DHHS that are not being addressed by current fraud efforts. The team met with the SmartCard project team to understand how the NC FACTS and the GBICC might be able to provide access to key data for the SmartCard pilot.

DHHS continues to review the necessary Data Access and Usage agreements as well other information security policies to enable data sharing to support the analysis of eligibility for services and payments across the enterprise.

III. Challenges

Agency Commitment

NC FACTS offers state agencies additional tools to provide added value to their fraud, waste and overpayment identification efforts using integrated statewide data. While agencies see value in the NC FACTS concept and express interest in participating in this enterprise initiative, they note that operational priorities inhibit their ability to commit resources to share their data and implement these business processes. Consequently, the pace of development of analytics to support their organizational anti-fraud efforts has not been at a level satisfactory to this Office.

Resource Limitations

There is no doubt that some agencies are limited from sharing data because of statutory, regulatory or legal challenges, but even when there are no legal impediments, limited agency resources continue to present a challenge to providing data. Despite the fact that executed data access and usage agreements are in place, the lack of agency staff resources to develop data extracts and provide business knowledge to support the required analysis continues to delay work effort toward developing fraud, waste and improper payment detection models.

To lessen the impact on technical resources within agencies, the NC FACTS program team has suggested that agencies consider the use of existing data extracts wherever possible. Existing extracts may not be as comprehensive as developing NC FACTS specific extracts, but they may include sufficient data to begin analysis and can be adapted as additional data needs are identified. The Division of Employment Security and the Department of Transportation are currently evaluating utilizing this approach.

Data Sharing

The data needed for effective enterprise analysis includes highly sensitive and secure information. The ability to protect Personal Identifying Information (PII), adhere to security and compliance requirements for the Health Information Portability and Accountability Act (HIPAA), and meet the constraints associated with other state and federal laws and regulations associated with tax information and employment data, is critical to sharing information across the enterprise. NC FACTS works closely with agencies to develop the required policies, procedures, contractual agreements, and memorandums of understanding or agreement necessary to define the parameters associated with data sharing of this key information within the State's fraud initiative.

Stringent application security, including physical security, user authentication, role-based security, and data encryption among others, are key components in the implementation of the enterprise fraud detection system. The ultimate success of this initiative is dependent on state agencies that partner and strive to find and implement appropriate policies and controls to enable data sharing. Some of the agencies who serve as data stewards of key

data sources have determined that statutory or regulatory provisions prevent the sharing of state data in their possession with this statewide initiative:

Department of Revenue

The Department of Revenue (DOR) houses sensitive information related to business and individual income, revenue, sales and tax information. This information is critical to analyzing a variety of areas including validating business and individual identities, reviewing provider claims and payments, analyzing recipient eligibility, and recognizing inconsistency in operations across the State's business areas. The Department of Revenue, in response to a data sharing inquiry, indicated that state statutes and regulations, specifically G.S. § 105-259, limits the disclosure of tax-related information. Tax information, defined in that statute, includes information contained on a tax return or obtained through an audit, information on whether or not an individual has filed a tax return or tax report, and a list of names, addresses, social security numbers, or similar information concerning taxpayers. Further, DOR indicated that federal regulations including Section 6103 of the Internal Revenue Code requires that federal returns and return information must be kept confidential except as specifically defined by statute. DOR noted that many of their data files co-mingle federal and state data which further complicate the sharing of information with the NC FACTS initiative. Section 7213 of the Internal Revenue Code provides that the unauthorized disclosure of tax information is a felony and is punishable by a fine of up to $5,000 and imprisonment of up to five years. Unauthorized inspection of tax information is a felony and is punishable by a fine of up to $1,000 and imprisonment of up to one year. The Department of Revenue believes that legislation is required to allow the use of State tax information in the fraud, waste and improper payment detection initiative. With the new data sharing legislation in Session Law 2012-142, HB 950, OSC will work with DOR to determine how DOR data may be incorporated into NC FACTS.

Department of Health and Human Services

Department of Health and Human Services (DHHS) stores key information about medical service providers, recipients, and claims, as well as other social services information. DHHS expressed concern about the NC FACTS initiative placing additional burden on their current fraud detection program resources. While NC FACTS may not engage in detailed fraud analysis within Medicaid, the data and results from current Medicaid efforts are vital to enabling linkages and an enterprise view of businesses and individuals. The NC FACTS team recognizes that regulatory requirements related to HIPAA protected information must be addressed

Program Resources for NC Fraud, Waste and Improper Payment Efforts

NC FACTS will provide data integration and analytics to identify suspect behavior, pattern anomalies, and errors in processing as the basis for detecting, investigating, recouping, and preventing fraud, waste and improper payments. A broader vision, however, is needed to develop a State culture focused on fiscal responsibility and accountability at all levels of State government.

North Carolina State Government serves its citizens and is responsible for ensuring that tax payer dollars are used in a fiscally appropriate manner. A focus on fraud, waste, and improper payment detection and prevention begins with fostering a culture within State government focused on accountability and transparency. To support this effort the following recommendations are provided:

Code of Conduct

Some, but not all, of North Carolina's State agencies have adopted an employee code of conduct. Consideration should be given to establishing a uniform North Carolina state employee code of conduct to ensure all state employees have a common, clearly defined set of guiding principles under to which to operate. The code of conduct sets the tone for employees and makes clear the expectation of a high standard of professional conduct.

Fraud Reporting

While data integration and analytics will provide the ability to systematically detect fraud through statistical analysis, pattern evaluation, and anomaly detection, information from other sources will continue to provide valuable information on fraudulent activity. Review of existing hotlines and tip reporting should be conducted to ensure that state government employees and the public have easy access to provide key information to state fraud program resources for review and investigation.

Consideration must also be given to the protection of state employees who provide information that they consider to be reasonable evidence of activity involving fraud, waste or improper payments. Consideration of additional language providing "whistle-blower" protection may be necessary to ensure the willingness of employees to report suspect behavior to the appropriate authorities.

Agency Resources

As the NC FACTS application identifies suspect data for review, agencies and the NC FACTS enterprise program must have the necessary resources to verify the accuracy of the findings, determine the cause of the findings, and identify and recommend resulting program changes to prevent future incidents. The Office of Internal Audit in the Office of State Budget and Management and the Statewide Internal Control Program in OSC have both identified the need for additional resources to support agencies and provide greater oversight for disbursement of state funds.

Incentives

As the automated fraud detection system is implemented and expanded throughout State agencies, OSC anticipates an increase in the number of incidents and types of fraud identified. Identifying fraud is only one step in the process of improving government operations. The ability to investigate and recover funds that were improperly expended -- and more importantly the ability to prevent future incidents of fraud -- is critical to achieving measureable success in improving government operations.

Except for the Courts, consideration should be given to providing a portion of the funds recovered from fraud, waste and improper payment analytics and recovery efforts to the employees, agencies and organizations as an incentive for the agency to provide the resources, equipment, and programs to analyze, investigate, and recover improperly expended funds. This funding could assist agencies with the essential resources required to adapt business policy and procedures, and improve information technology systems to identify and prevent improper payments.

Measurement of Benefits Realized

As previously mentioned, a number of fraud detection initiatives exist throughout state government. To distinguish benefits associated with the implementation of the enterprise fraud detection initiative from existing efforts will prove challenging. In order to accurately measure and report on benefits realized, OSC will work with partner agencies and organizations to identify ways to supplement existing detection efforts with enterprise data and analytics.

As fraud detection improves the ability of state agencies to adapt processes and controls to prevent fraud, quantitative reporting of prevention efforts will consider historical fraud statistics as well as measured payments that were flagged and stopped prior to payment.

Maintenance of Analytical Models

Enterprise data and robust analytical tools will identify data patterns and anomalies in order to detect fraudulent and improper payments. With advanced analytics, it is likely that the number of identified data anomalies will increase significantly. Because State agencies and organizations have limited resources to review, investigate and recover improper payments, it is critical that the automated fraud detection system provide a feedback mechanism to continually refine analytic models. As investigators determine which cases involve fraud from cases that involve erroneous payments, the models can be adjusted to better identify high risk cases. Feedback will also allow the models to be refined so that suspect criteria are more specific leading to a reduction in the number of "false

positive" cases. The feedback can also provide information to hold and subject suspect payments to a review process prior to expending funds.

As the State improves its ability to detect and prevent fraud, individuals who commit fraud will find alternative methods of gaining improper access to payments and services. All analytic models must be flexible to ensure the State's fraud detection ability maintains pace with the creativity of those attempting to defraud the State.

IV. Budget

Session Law 2011-145, HB 200, authorized funding of $9M in the biennium budget for the development of an automated fraud, waste and improper payment data integration program. These funds support OSC's state project team staffing and expenses ($1M) as well as contractual services for the design, development and implementation of data integration and business analytic models for fraud detection ($8M). To ensure the public-private partnership of this initiative, the State's data integration vendor is required to contribute resources in the amount of $5M over the next two years ($10M total). The vendor contribution will provide hosting hardware and technical environment infrastructure, software, support and services for design, development and implementation of data integration and business analytic model development.

Because data sharing challenges significantly inhibited data analysis and development in FY 2012, to ensure adequate progress is being made toward reaching the General Assembly's public/private partnership mandate, OSC negotiated a contract extension with the vendor for an additional full year at no additional cost. Payments have been delayed accordingly.

To support the fraud analytics initiative, however, recurring funding is necessary to establish permanent positions for the skilled program resources and to support the analytics licensing and development services will be required to sustain the automated fraud detection program efforts.

Projected Budget

	FY 2012	FY 2013
Fraud Detection Funding		
State Funding	$1,500,000	$7,500,000
Vendor Financial Contribution	5,000,000	$5,000,000
	$6,500,000	**$12,500,000**
Fraud Detection Expenditures		
State Project Team Expenditures	$500,000	$500,000
Vendor Contracted Services Payment - December, 2011	1,000,000	
Vendor Contracted Services Payment - July, 2012*		3,000,000
Vendor Contracted Services Payment - December, 2012*		3,000,000
Vendor Contracted Services Payment - June, 2013		1,000,000
Vendor Hosting, Software and Contracted Services Contribution	5,000,000	5,000,000
NC FACTS Total	**$ 6,500,000**	**$ 12,500,000**

* Vendor Service payment delayed

Actual Expenditures/Vendor Contributions

As of May 31, 2012	FY 2012 Actual	FY 2013 Actual
State Fraud Detection Funding		
State Funding	$1,500,000	$7,500,000
Carryover from FY 2012		497,228
Total Budgeted Funds Available	**$ 1,500,000**	**$ 7,997,228**
Expenditures		
State Project Team Expenditures	$2,772	$318,316
Vendor Payments to Date	1,000,000	
Scheduled Vendor Payment - June 2013		3,000,000
Total Expenditures	**$ 1,002,772**	**$ 3,318,316**
Total Budget Funds Remaining	**$ 497,228**	**$ 4,678,912**
Vendor Fraud Detection Contribution		
Vendor Financial Contribution - Planned	5,000,000	5,000,000
Carryover from FY 2012		768,355
Total Planned	**$ 5,000,000**	**$ 5,768,355**
Vendor Fraud Detection Expenditures - Actual	4,231,645	6,340,153
Total Contributions Remaining	**$ 768,355**	**$ (571,798)**

Budget Expansion

The NC FACTS program budget funding is funded through June 30, 2013. A budget expansion request was submitted to support the continued development and expansion of the program through the next biennium.

I. Next steps

- Continue work on the NC FACTS pilot program areas:
  - Operationalize and expand the unemployment insurance benefit and employer filing fraud analysis
  - Continue State Health Plan of North Carolina business requirements definition and analysis
  - Initiate Department of State Treasurer – Division of Retirement data
  - Feeds, business requirements definition and analysis
  - Continue analysis of integrated data
    - SOS information
    - SSA Master Death File
    - NCAS vendor and payments data
    - BEACON payroll and time data
    - DHHS Center for Health Statistics Deceased Records
    - DMV License and Vehicle Registration Records
  - Provide program recommendations for recovery and prevention of identified incidents
  - Report realized benefits

- Identify data sharing statutory and regulatory challenges and recommendations for addressing these challenges.

- Identify additional business areas of interest and plan for program expansion.

Criminal Justice Law Enforcement Automated Data Services (CJLEADS)

I. Background

In 2008, the North Carolina General Assembly initiated the Criminal Justice Data Integration Program with the mandate to create a statewide criminal justice system designed to save time, save money, and save lives. Since the project's inception, the Office of the State Controller (OSC) has worked with SAS as a vendor partner in collaboration with North Carolina's criminal justice organizations to develop and implement the Criminal Justice Law Enforcement Automated Data Services (CJLEADS) system.

Consistent with the General Assembly's intent to serve criminal justice professionals and improve the safety of North Carolina's citizens, CJLEADS has two primary objectives:

1. To provide a comprehensive view of an offender through a single application, allowing for positive identification of an offender through a photographic image.

2. To provide an "offender watch" capability to alert criminal justice professionals when an offender has a change in status.

CJLEADS is now used statewide by over 26,500 criminal justice users including judges, prosecutors, clerks of court, magistrates, prison officials, probation and parole officers and law enforcement at the State, federal and local levels. The CJLEADS team maintains regular communications with end users and deploys two to four application releases each year to ensure the application is continuously improved to meet the needs of the criminal justice community.

OSC maintained tight fiscal control over the CJLEADS development to ensure that state funds have achieved maximum value. The initial pilot development and statewide deployment expenditures were $24,620,475 or approximately 9% under the original budget estimate of $27,000,000.

In FY 2011-2012, recurring funding for CJLEADS annual operating expenses was reduced from $9 million to $6,632,737. That year the operating budget was supplemented with remaining CJLEADS special project funds. In FY 2012-2013 the General Assembly authorized $2,379,000 in non-recurring funding to support current operations, migration to a more robust enterprise database system, and development of enhanced functionality. Since the initial pilot, CJLEADS has deployed nine (9) production releases, each one providing functional or data enhancements in response to the needs of the criminal justice community. The proposed FY 2013-2015 budget of $6.6 million, with no expansion, will result in continued operations and maintenance of the CJLEADS with minimal future functional or data enhancements.

II. CJLEADS Statewide Operations

A. Business Operations

CJLEADS is being used statewide by over 26,500 criminal justice professionals. The CJLEADS Business Operations Team provides on-boarding assistance to criminal justice organizations, offers regular training classes and provides 24x7 online and telephone support for all CJLEADS end users and user administrators.

As of June 3, 2013:

- 520 federal, state, and local law enforcement organizations are licensed to use CJLEADS.
- Over 26,500 end users have been trained in more than 2,186 CJLEADS classes, including classroom, web-based classes and night classes.
- Over 82 certified "Train-the-Trainers" have conducted 755 classes for their organizations.
- Over 100 user inquiries are managed weekly by CJLEADS support on a 24x7x365 basis.

B. Usage

Since initial deployment in June 2010, criminal justice professionals have conducted over 18.5 million searches and accessed nearly 15.3 million offender and DMV records. Over 9,600 users access CJLEADS each week.

In December 2012, CJLEADS released the new DMV Partial Plate functionality that allows law enforcement officers (LEO) to search for vehicles using partial license tag numbers, partial vehicle identification numbers (VINs) and other vehicle characteristics for investigative purposes. Before CJLEADS provided this capability, an officer needing to perform this type of vehicle search would submit a request in writing to the Driver and Vehicle Services section of DMV. DMV resources would develop the appropriate programming code, run a mainframe job using CPU time and resources, and generate a paper report to provide to the requesting officer, often taking one or more business days. Using CJLEADS, a LEO now can perform the search and receive results in minutes improving access to information for their investigations.

The cost of developing the DMV Partial Plate search was approximately $81,000. Based on DMV's estimated cost to generate a manual vehicle search report and the number of CJLEADS vehicle searches performed since the new functionality was implemented, the CJLEADS vehicle searches to date have produced an estimated cost avoidance of $76,000. This savings offsets 94% of the cost of development in just six months. The number of CJLEADS vehicle searches has increased dramatically over the number of requests typically processed through the DMV, most likely because officers see the improved ability and value associated with getting this key information immediately to assist in their investigations.

C. Auditing

In accordance with CJLEADS policy, the CJLEADS Business Operations team conducts annual audits of all licensed end user organizations. Each agency receives a packet containing CJLEADS user lists, usage reports, and agency contact update forms. Agencies review the CJLEADS usage and end user reports, verify their authorized end users and notify of any suspect usage or access. The Business Operations Team successfully completed the first annual cycle and the second year is underway and on schedule.

In addition to the annual audit process, the CJLEADS Business Operations team periodically receives audit investigation requests from agencies related to possible fraudulent usage of the system or an agency's internal investigation process. The Business Operations Team has assisted agencies with 10 requests so far in 2013.

III. Application Releases

The CJLEADS Project team continues to work with end users, data source agencies, and SAS to incorporate data and enhance functionality deemed critical to meeting the mission of providing a reliable, complete, and simple-to-use application to serve law enforcement and the courts and thereby improve the safety of our State, its communities, and citizens.

Release 9 was deployed on May 2, 2013. Release 9 enhanced existing functionality and refined key reports.

- **Real-time interface with the Statewide Warrant Repository**

  CJLEADS integrates court records and outstanding processes in the nightly batch data loads. When users view an offender record, information about the outstanding process could be 24-36 hours old. With the development of the real-time interface to the Statewide Warrant Repository, CJLEADS is able to verify the status of any existing outstanding processes whenever the end user views the offender's record. In addition, the CJLEADS user may view any new processes issued for the offender since the last CJLEADS update. This feature provides critical, real-time information to law enforcement officers.

- **Links to NC General Statutes on the AOC Offense Code Tab**

  To provide easy access to key offense information, a page providing links to the General Statutes for all AOC offense codes was added to AOC Offense Codes page of the application. The user can now view statutory language related to any given offense.

- **Other enhancements include**
  - The DMV search-results-screen was modified to improve the placement of key status fields, saving law enforcement officers valuable time when reviewing results.

- Enhancements were made to the Watchlist, Alerts and Notifications print capabilities to allow users to the save to Excel for sorting and managing the data
- Addition of a link to the C-National Data Base – Justice Exchange website providing quick access to an outside criminal justice resource
- Addition of an optional notes field to allows users to record information about a particular search which may be helpful later during investigations as well as during user audits

IV. CJLEADS Database Upgrade

The CJLEADS application is currently operating on Asterdata database technology. As the CJLEADS application has matured, the technical team has encountered limitations of the Asterdata technology resulting in increased support issues, performance deficiencies during defined periods of the day, and limited ability to work with large datasets. In addition, the acquisition of Asterdata by another technology vendor creates an uncertain future for the product.

The General Assembly provided non-recurring funding in FY 2012-2013 to complete a technology upgrade to Oracle Exadata technology. The migration is in progress and scheduled for completion during summer 2013. Using Oracle Exadata technology, CJLEADS is expected to benefit from improved performance levels in extracting, transforming and loading data as well as in the response times for inquiries and reporting. In addition, the new technology will provide an enterprise foundation that supports the ability to add new data and functionality to meet future business needs.

V. Future Application Enhancement

Consistent with the legislative mandate to provide a comprehensive profile of an offender, CJLEADS strives to continuously improve the application with the development of additional functionality and data. With no expansion funding, minimal data and functional enhancements over the next two years will be produced.

The following functionality is currently under development and will be deployed in upcoming releases of CJLEADS:

A. Release 10 – Scheduled for Fall 2013

1. **Division of Community Corrections (DCC) Watch List** will generate probation watch lists and alerts for DCC officers who are responsible for supervising/monitoring active probationers, active absconders and expired absconders.
2. **Wildlife Hot Keys** will implement hot keys to enable wildlife officers to quickly access wildlife license and vessel numbers checks, much like the existing functionality for DMV licenses and plates.

3. **Group Watch List Member Notification** will integrate the ability for a CJLEADS group watch list member to send a notification to other group watch list members.
4. **Pretrial Report** will automate a current manual process of aggregating certain information in preparation for a court case as requested by Pretrial Services.
5. **U.S. Courts Report** will generate criminal history chronologically based on individual offenders who have court case alerts within a specified date range.
6. **Pending Offenses Report** will generate a list of offenders based on a selected offense category that have a pending charges and an upcoming court date for that offense category. Offense categories include Breaking and Entering, Larceny/Theft, Drug Offenses, Assault and Battery, Kidnapping, Gang, and Manslaughter etc.

B. Future Functionality

The following areas are being reviewed and/or preparatory work has begun for future releases of the CJLEADS application:

1. Federal Interface – Division of Criminal Information (DCI)

Both the courts and law enforcement have emphasized the critical need for a federal interface to allow users access to federal and other states' information via CJLEADS. CJLEADS, collaborating with the State Bureau of Investigation, North Carolina's CJIS Security Agency, and the North Carolina Department of Justice (NC DOJ) Information Technology Division, is developing policies and protocols to allow access to information from the Criminal Justice Information System (CJIS) via the DCI switch.

In addition, the development of the DCI interface will allow for Hot File status (a flag to indicate whether or not there is or is not information about wanted persons, stolen vehicles and stolen weapons on file with the DCIN) to be available for all CJLEADS LEOs, regardless of DCI certification.

There are a number of security and policy issues that must be addressed to allow CJLEADS to develop an interface to federal systems. CJLEADS requested an ORI from the FBI to facilitate access to the CJIS data needed for this effort which was not granted. CJLEADS is working with the SBI to determine the best method to comply with FBI security policy so that work toward completion of this interface can continue.

A critical component to deploying the DCI web service is Advanced Authentication (AA). (See previous Legislative Report for more information). ITS has an RFP to determine the best enterprise solution for AA that can integrate with NCID. All CJLEADS users will need AA access after completion of the DCI web services.

2. Business Analytics

With the data integrated into CJLEADS, there is great potential to mine the data for statistical analysis and reporting. Court and law enforcement personnel have suggested many opportunities to leverage the information in CJLEADS to improve efficiencies and effectiveness throughout the criminal justice community. The project team will work with business users to determine requirements for data analytics.

The kinds of analytics under consideration for development include trending related to recidivism, and relationships between offenders as well as other analytics based on needs and data availability.

3. NC-DEx

CJLEADS is partnering with the NC Department of Justice Information Technology Division to establish a web interface between the North Carolina Data Exchange (NC-DEx) – formerly known as CAPTURES. This interface to the comprehensive incidents database will enable the accurate and timely sharing of law enforcement data and allow authorized NC-DEx users to log into that system from within CJLEADS.

4. **Alert for Confidential License Plates –** Law enforcement has requested an alert mechanism to enable automatic notification anytime a DMV vehicle check is run against a confidential license plate.

5. Facial Recognition

The ability to positively identify a suspect, offender, or unknown person in the field is critical to law enforcement. The CJLEADS team, in collaboration with DMV, will analyze the ability to capture a photograph in the field and find potential matches for identification purposes by leveraging the existing DMV facial recognition technology.

VI. CJLEADS Challenges

The integration of data across multiple and often disparate applications brings with it many challenges. The following issues have been identified:

A. Funding Availability

The original CJLEADS pilot estimate was approximately $2 million. With the success of the initial pilot application, the General Assembly subsequently adopted legislation directing OSC to enhance the CJLEADS pilot to a 24x7x365 highly available production application, continue the development of additional data and functionality, and deploy the application to criminal justice professionals statewide. The total estimate for the three-year cost estimates, including initial pilot startup costs in FY 2008-09, was $27 million to support 30,000 criminal justice professionals statewide. The total cost of statewide deployment was $24,620,475, approximately 9% under budget. As consistently reported, annual operations and maintenance costs are approximately $8 million.

Actual/Estimated Costs

	FY 2008-2009	FY 2009-2010	FY 2010-2011	FY 2011-2012	FY 2012-2013	FY 2013-2014
	Pilot	Production Development and Statewide deployment				
	Actual	Actual	Actual	Actual	Estimated Cost	Estimated Cost
SAS Hosted Solution						
State Operations	$128,091	$390,601	$1,415,978	$1,594,888	$2,429,302	$1,950,000
Development/Hosting/Software	$2,000,000	$7,252,426	$6,460,491	$5,378,000	$6,598,000	$6,050,000
Total	**$2,128,091**	**$7,643,027**	**$7,876,469**	**$6,972,888**	**$9,027,302**	**$8,000,000**

The FY 2012-2013 recurring appropriation for CJLEADS is $6.6 million. In addition, the General Assembly appropriated $2.38 million in non-recurring funds to enable the Oracle database upgrade and continued application enhancement. An expansion request was submitted to restore funding to the estimated annual operating costs of $8 million. The additional funds will be needed for the increased hosting and support costs with the Oracle data base technology, on-going operations, and protection of the State's investment in CJLEADS by enhancing the application to keep pace with evolving technology.

With the proposed FY 2013-2015 funds of $6.6 million, CJLEADS will continue operations with minimal ability to add data and functionality to the application.

The following chart provides an explanation of the funding and expenditures:

Funding/Expenditures

As of May 31, 2013	FY 2012-2013 Budget	Actuals	Available Balance
CJLEADS Funding			
Recurring Funding	$6,648,302		
One-time Project Funding	$2,379,000		
	$9,027,302		
CJLEADS Expenditures			
Total Project FY 2012 - 2013			
State Project Team Expenditures	$2,429,302	$1,517,890	
Hosting Contract Services	1,550,000	1,550,000	
Development/Support Contract Services	2,048,000	1,843,200	
SAS ELA Renewal	2,000,000	2,000,000	
Oracle Upgrade Hosting Costs	1,000,000	1,000,000	
CJLEADS Total	**$ 9,027,302**	**$ 7,911,090**	**$ 1,116,212**

VII. Next Steps

- Oracle Migration – Summer 2013
- Release 10 – Fall 2013
- Continue planning for future enhancements
- Continue vendor hosting and support
- Business Operations will:
    - Continue training
    - Complete the next cycle of auditing
    - Continue to provide after-hours customer service support
- Document areas for continuous improvement and future enhancements for the CJLEADS application

Appendices

Appendix A

Session Law 2012-142, HB 950

ENHANCE ENTERPRISE-LEVEL BUSINESS INTELLIGENCE TO INCREASE EFFICIENCY IN STATE GOVERNMENT

SECTION 6A.7A.(a) Creation of Initiative. –

(1) Creation. – The enterprise-level BI initiative (initiative) is established in the Office of State Controller. The purpose of the initiative is to support the effective and efficient development of State agency BI capability in a coordinated manner and reduce unnecessary information silos and technological barriers. The initiative is not intended to replace transactional systems, but is instead intended to leverage the data from those systems for enterprise-level State BI.

The initiative shall include a comprehensive evaluation of existing data analytics projects and plans in order to identify data integration and BI opportunities that will generate greater efficiencies in, and improved service delivery by, State agencies. The Office of State Controller may partner with current vendors and providers to assist in the initiative. However, to limit the cost to the State, the Office of the State Controller shall use current licensing agreements wherever feasible.

(2) Application to State government. – The initiative shall include all State agencies, departments, and institutions, including The University of North Carolina.

(3) Governance. – The State Controller shall lead the initiative established pursuant to this section. The Chief Justice of the North Carolina Supreme Court and the Legislative Services Commission each shall designate an officer or agency to advise and assist the State Controller with respect to implementation of the initiative in their respective branches of government. The judicial and legislative branches shall fully cooperate in the initiative mandated by this section in the same manner as is required of State agencies.

SECTION 6A.7A.(b) Government Business Intelligence Competency Center. –

(1) GBICC established. – There is established in the Office of the State Controller the Government Business Intelligence Competency Center (GBICC). GBICC shall assume the work, purpose, and resources of the current data integration effort in the Office of the State Controller and shall otherwise advise and assist the State Controller in the management of the initiative. The State Controller shall make any organizational changes necessary to maximize the effectiveness and efficiency of GBICC.

(2) Powers and duties of the GBICC. – The State Controller shall, through the GBICC, do all of the following:

a. Continue and coordinate ongoing enterprise data integration efforts, including:

1. The deployment, support, technology improvements, and expansion for CJLEADS.

2. The pilot and subsequent phase initiative for NC FACTS.
3. Individual-level student data and workforce data from all levels of education and the State workforce.
4. Other capabilities developed as part of the initiative.

b. Identify technologies currently used in North Carolina that have the capability to support the initiative.

c. Identify other technologies, especially those with unique capabilities that could support the State's BI effort.

d. Compare capabilities and costs across State agencies.

e. Ensure implementation is properly supported across State agencies.

f. Ensure that data integration and sharing is performed in a manner that preserves data privacy and security in transferring, storing, and accessing data, as appropriate.

g. Immediately seek any waivers and enter into any written agreements that may be required by State or federal law to effectuate data sharing and to carry out the purposes of this section.

h. Coordinate data requirements and usage for State BI applications in a manner that (i) limits impacts on participating State agencies as those agencies provide data and business knowledge expertise and (ii) assists in defining business rules so the data can be properly used.

i. Recommend the most cost-effective and reliable long-term hosting solution for enterprise-level State BI as well as data integration, notwithstanding Section 6A.2(f) of S.L. 2011-145.

SECTION 6A.7A.(c) Implementation of the Enterprise-Level BI Initiative. –

(1) Phases of the initiative. – The initiative shall commence no later than August 1, 2012, and shall be phased in accordance with this subsection. The initiative shall cycle through these phases on an ongoing basis:

a. Phase I requirements. – In the first phase, the State Controller through GBICC shall:

1. Inventory existing State agency BI projects, both completed and under development.

2. Develop a plan of action that does all of the following:

I. Defines the program requirements, objectives, and end state of the initiative.

II. Prioritizes projects and stages of implementation in a detailed plan and benchmarked timeline.

III. Includes the effective coordination of all of the State's current data integration initiatives.

IV. Utilizes a common approach that establishes standards for BI initiatives for all State agencies and prevents the development of projects that do not meet the established standards.

V. Determines costs associated with the development effort and identifies potential sources of funding.

VI. Includes a privacy framework for BI consisting of adequate access controls and end user security requirements.

VII. Estimates expected savings.

3. Inventory existing external data sources that are purchased by State agencies to determine whether consolidation of licenses is appropriate for the enterprise.

4. Determine whether current, ongoing projects support the enterprise-level objectives.

5. Determine whether current applications are scalable, or are applicable for multiple State agencies, or both.

b. Phase II requirements. – In the second phase, the State Controller through the GBICC shall:

1. Identify redundancies and determine which projects should be discontinued.

2. Determine where gaps exist in current or potential capabilities.

c. Phase III requirements. – In the third phase:

1. The State Controller through GBICC shall incorporate or consolidate existing projects, as appropriate.
2. The State Controller shall, notwithstanding G.S. 147-33.76 or any rules adopted pursuant thereto, eliminate redundant BI projects, applications, software, and licensing.

3. The State Controller through GBICC shall complete all necessary steps to ensure data integration in a manner that adequately protects privacy.

(2) Commencement of projects. – Subject to the availability of funds, and subsequent to the submission of the written report required by sub-subdivision a. of subdivision (1) of subsection (e) of this section, the State Controller shall begin projects to carry out the purposes of this section no later than November 1, 2012. The State Controller may also expand existing data integration or BI contracts with current data integration efforts, as appropriate, in order to implement the plan required by this section in accordance with the schedule established and the priorities developed during Phase I of the initiative, and may use public-private partnerships as appropriate to implement the plan.

SECTION 6A.7A.(d) Funding. **–**

(1) Allocation. – Of the funds appropriated from the General Fund to the General Assembly for the 2011-2013 fiscal biennium, the sum of five million dollars ($5,000,000) shall be used to fund the initiative established by this section. The Office of the State Controller shall use up to seven hundred fifty thousand dollars ($750,000) to cover the cost of administering the initiative.

(2) Federal funds. – The Office of State Controller, with the support of the Office of State Budget and Management, shall identify and make all efforts to secure any matching funds or other resources to assist in funding this initiative.

(3) Use of savings. – Savings resulting from the cancellation of projects, software, and licensing, as well as any other savings from the initiative, shall be returned to the General Fund and shall remain unexpended and unencumbered until appropriated by the General Assembly in a subsequent fiscal year. It is the intent of the General Assembly that expansion of the initiative in subsequent fiscal years be funded with these savings and that the General Assembly appropriate funds for projects in accordance with the priorities identified by the Office of the State Controller in Phase I of the initiative.

SECTION 6A.7A.(e) Reporting. **–**

(1) Routine reports. – The Office of the State Controller shall submit and present the following reports:

a. By no later than October 1, 2012, a written report on the implementation of Phase I of the initiative and the plan developed as part of that phase to the Chairs of the House of Representatives Appropriations and Senate Base Budget/Appropriations Committees, to the Joint Legislative Oversight Committee on Information Technology, and to the Fiscal Research Division of the General Assembly. The State Controller shall submit this report prior to implementing any improvements, expending funding for expansion of existing BI efforts, or establishing other projects as a result of its evaluations.

b. By February 1, 2013, and quarterly thereafter, a written report detailing progress on, and identifying any issues associated with, State BI efforts.

(2) Extraordinary reports. – The Office of the State Controller shall report the following information as needed:

a. Any failure of a State agency to provide information requested pursuant to this section. The failure shall be reported to the Joint Legislative Committee on Information Technology and to the Chairs of the House of Representatives Appropriations and Senate Base Budget/Appropriations Committees.

b. Any additional information to the Joint Legislative Commission on Governmental Operations and the Joint Legislative Oversight Committee on Information Technology that is requested by those entities.

SECTION 6A.7A.(f) Duties of State Agencies. –

(1) Duties of State agencies. – The head of each State agency shall do all of the following:

a. Grant the Office of the State Controller access to all information required to develop and support State BI applications pursuant to this section. The State Controller and the GBICC shall take all necessary actions and precautions, including training, certifications, background checks, and governance policy and procedure, to ensure the security, integrity, and privacy of the data in accordance with State and federal law and as may be required by contract.

b. Provide complete information on the State agency's information technology, operational, and security requirements.

c. Provide information on all of the State agency's information technology activities relevant to the State BI effort.

d. Forecast the State agency's projected future BI information technology needs and capabilities.

e. Ensure that the State agency's future information technology initiatives coordinate efforts with the GBICC to include planning and development of data interfaces to incorporate data into the initiative and to ensure the ability to leverage analytics capabilities.

f. Provide technical and business resources to participate in the initiative by providing, upon request and in a timely and responsive manner, complete and accurate data, business rules and policies, and support.

g. Identify potential resources for deploying BI in their respective State agencies and as part of the enterprise-level effort.

h. Immediately seek any waivers and enter into any written agreements that may be required by State or federal law to effectuate data sharing and to carry out the purposes of this section, as appropriate.

SECTION 6A.7A.(g) Miscellaneous Provisions. **–**

(1) Status with respect to certain information. – The State Controller and the GBICC shall be deemed to be all of the following for the purposes of this section:

a. With respect to criminal information, and to the extent allowed by federal law, a criminal justice agency (CJA), as defined under Criminal Justice Information Services (CJIS) Security Policy. The State CJIS Systems Agency (CSA) shall ensure that CJLEADS receives access to federal criminal information deemed to be essential in managing CJLEADS to support criminal justice professionals.

b. With respect to health information covered under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, and to the extent allowed by federal law:

1. A business associate with access to protected health information acting on behalf of the State's covered entities in support of data integration, analysis, and BI.

2. Authorized to access and view individually identifiable health information, provided that the access is essential to the enterprise fraud, waste, and improper payment detection program or required for future initiatives having specific definable need for the data.

c. Authorized to access all State and federal data, including revenue and labor information, deemed to be essential to the enterprise fraud, waste, and improper payment detection program or future initiatives having specific definable need for the data.

d. Authorized to develop agreements with the federal government to access data deemed to be essential to the enterprise fraud, waste, and improper payment detection program or future initiatives having specific definable need for such data.

(2) Release of information. – The following limitations apply to (i) the release of information compiled as part of the initiative, (ii) data from State agencies that is incorporated into the initiative, and (iii) data released as part of the implementation of the initiative:

a. Information compiled as part of the initiative. – Notwithstanding the provisions of Chapter 132 of the General Statutes, information compiled by the State Controller and the GBICC related to the initiative may be released as a public record only if the State Controller, in that officer's sole discretion, finds that the release of information is in the best interest of the general public and is not in violation of law or contract.

b. Data from State agencies. – Any data that is not classified as a public record under G.S. 132-1 shall not be deemed a public record when incorporated into the data resources comprising the initiative. To maintain confidentiality requirements attached to the information provided to the State Controller and GBICC, each source agency providing data shall be the sole custodian of the data for the purpose of any request for inspection or copies of the data under Chapter 132 of the General Statutes.

c. Data released as part of implementation. – Information released to persons engaged in implementing the State's BI strategy under this section that is used for purposes other than official State business is not a public record pursuant to Chapter 132 of the General Statutes.

SECTION 6A.7A.(h) G.S. 75-66(d) reads as rewritten:

"(d) Nothing in this section shall:

(1) Limit the requirements or obligations under any other section of this Article, including, but not limited to, G.S. 75-62 and G.S. 75-65.

(2) Apply to the collection, use, or release of personal information for a purpose permitted, authorized, or required by any federal, State, or local law, regulation, or ordinance.

(3) Apply to data integration efforts to implement the State's BI strategy as provided by law or under contract."

Appendix B

GDAC Data Sources

NCAS	*BEACON*	*Division of Employment Security*
Purchasing Card Transactions	*Employee and Position Data*	*Benefits Payment Information*
Payment Data	*Employee Earnings Information*	*Case Management Data*
Vendor Information		*Employer Tax Information*
CJLEADS	*State Employees Health Plan*	*Division of Motor Vehicles*
DPS - Prison	*Medical Claims Detail*	*Driver's License Data*
DPS - Probation	*Pharmacy Claims Data*	*Vehicle Registration Data*
DPS – Local Jail	*Provider and Member Information*	
AOC - Criminal Court Records	*Secretary of State*	*Industrial Commission*
DOJ - Concealed Handgun Data	*Corporation Information*	*Workers Compensation Insurance*
DOJ - Sex Offender Registry	*UCC Information*	
Wildlife – Web Service	*DHHS - Center for Health Statistics*	*Other – External Sources*
	Vital records – Deceased Information	*Bank of America P-Card Data*
Future Data Sources		*Social Security Death Master File*
Retirement Information		
Unclaimed Property		
Education		
DHHS		