Confidentiality, Integrity, Availability: Georgia's Prescription for a Good Night's Sleep

Georgia Digital Academy on Data Security

Final Report

Prepared by:

Participants of the
Georgia Digital Academy on Data Security

Prepared for:

Robert Woodruff, Director
Technology Office
Georgia Technology Authority
Atlanta, Georgia

Compiled and Edited by:

Doris R. Konneh, Georgia Technology Authority
Walter Tong, Georgia Technology Authority
Richard Halstead-Nussloch, Southern Polytechnic State University

TABLE OF CONTENTS

1. Abstract 3
2. Summary 5
3. Introduction 6
    3.1 Purpose 6
    3.2 Scope 6
    3.3 Background 7
    3.4 Pertinent Data Security Legislation and Programs 8
    3.5 XML and XML Schema 13
    3.6 GTA Policies, Standards and Guidelines 13
    3.7 Major Issues in Data Security 13
    3.8 Related Issues in Data Security 14
4. Methods and Procedures 15
    4.1 Facilitated, Interactive Sessions 15
    4.2 Continuous Improvement and Web-based Research 15
    4.3 An Ongoing Group Activity: Planning for Data Security 16
    4.4 Subject Matter Experts (SMEs) 16
    4.5 Division into Two Groups of Interest 16
5. Results and Discussion 18
    5.1 Findings 18
    5.2 Significance of Findings 20
    5.3 Implications of Findings 21
    5.4 Recommendations 22
6. References and Bibliography 23

APPENDIX A - Data Categorization Standard 25
APPENDIX B - Data Categorization Advice Document 31
APPENDIX C - Glossary 41
APPENDIX D - Distribution List 45
APPENDIX E - The Privacy Act of 1974 46
APPENDIX F- Georgia Open Records Act 68
APPENDIX G - How to Remain Open in a Closed Standards World 83
APPENDIX H - Privacy and Access Conference Agenda 86

1. ABSTRACT

This final report is the result of a collaborative effort of the state agencies participating in the Georgia Digital Academy on Data Security (GDADS) session held at Southern Polytechnic State University in 2003. Also, representatives of the Georgia Technology Authority's Technology Office, Office of Information Security, and Southern Polytechnic State University staff made significant contributions to the academy session and to the report. The report is a summary of the activities and the resulting recommendations concerning the GDADS' attempts to address the need for data security standards throughout Georgia state government. In addition to such recommendations, the ultimate goal of the GDADS is to support the development of an infrastructure to align Georgia with the Federal Enterprise Architecture. This alignment is required to ensure that a secure environment is implemented to facilitate the sharing of sensitive data among state agencies, their partners, and the federal government, while providing protection of critical data assets.

The report includes the following major elements that pertain to the GDADS session:

- Overview
- Purpose and Goals
- Issues
- Proposed Solutions
- Focus Areas
    - Data Mapping
    - Data Categorization
    - Technical Standards for data security
    - Implementation Plans for data Security
    - Privacy and Access

A brief description of applicable data security standards, federal regulations, and related issues is also provided.

The GDADS participants and the authors/editors of this report extend our appreciation to the following people and groups. The discussions and interactions have been valuable to each of us personally and professionally and should prove beneficial to citizens, employees and every state agency in our continual efforts in data security:

- **Southern Polytechnic State University** for their hospitality and the use of facilities. We especially thank Dean Dawn Ramsey and the staff of the Extended University department for their assistance and support.
- **Georgia Technology Authority** for its sponsorship. We especially thank Robert Woodruff and Tom Wade for their vision and unwavering support of the value of the digital academy approach.

- **Archives Division/Secretary of State Office** for their support. Thanks to them, we were able to benefit from the knowledge and expertise of consultant Charles Dollar.
- **Dr. Charles Dollar** for spending time in educating us about some of the major issues in data security.
- **Privacy and Access in Georgia e-Government Conference** sponsored by the Archives Division. This was a valuable adjunct to the academy and the opportunity to participate is much appreciated.
- **Department of Audits** for their support and participation as an advisor to the academy.

2. SUMMARY

The Federal Government is addressing the issue of lack of consistent standards relating to information and information processing systems. The E-Government Act of 2002 (Public Law 107-347), passed by the one hundred and seventh Congress and signed into law by the President in December 2002, recognized the importance of information security standards to the economic and national security interests of the United States. The Federal Information Security Management Act of 2002 tasked the National Institute of Standards and Technology with developing standards to be used by all Federal agencies to categorize all information and information systems collected or maintained by each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels.

Similar standards are needed at the state Government level. The lack of implemented data security standards can jeopardize the information and information systems needed by Georgia state agencies to accomplish their assigned missions that include: the protection of assets and individual privacy, fulfillment of legal responsibilities, and execution of day-to-day business operations. Standards are also needed to ensure that the necessary infrastructure is implemented that will allow state agencies to share critical data at the federal, state, and local levels.

As a result of the significant issues associated with protecting the state's information and information systems, the need for agencies to share sensitive information, and the lack of a plan for the implementation of a secure infrastructure to accomplish this goal, the Georgia Digital Academy on Data Security recommends the following course of action:

- Continue to provide a forum for state agencies to collaborate and develop solutions to common issues associated with information and data security.
- Develop and implement an enterprise information security standard for data categorization based on the recommendations of the GDADS as contained in its advice document (See Appendix B).
- Support the rollup of agency data categorization implementation plans to the state enterprise level.
- Partner with agencies to facilitate a data security work group to develop a long- term strategy and implementation plan that addresses the needs of state and agency business programs.
- Develop and implement state enterprise information security standards to support technology and infrastructure requirements that are in line with the Federal Enterprise Architecture.

3. INTRODUCTION

The Georgia Digital Academy is a prime catalyst for state agencies to come together to develop technical solutions to common business problems. It is housed on the campus of Southern Polytechnic State University (SPSU) in Marietta.

During the academy's session on data security, participants enhanced their knowledge and capability by working on mapping and categorizing data, developing technical standards, and designing an implementation plan appropriate for their state agency. They helped identify and propose best practices for data security to be used throughout Georgia state government and achieved their primary goal of establishing trust levels to protect the state's data and information based upon the currently available security requirements.

3.1 Purpose

The goals of the academy on data security were to:

- facilitate collaboration and education among state agencies to enhance data security in Georgia
- accelerate the identification and standardization of best practices for data security throughout state government
- develop plans and solutions to meet the business requirements for data security of state agencies

3.2 Scope

The scope of the academy session on data security was to initiate the development of a statewide approach to data security. This approach included a high-level map of current applications, a matrix of data categories annotated for security levels, an initial standard for data security, and a template for an implementation plan.

Specific activities included:

- learning more about data security and its technology and role in Georgia
- mapping data held by each agency into a security framework
- categorizing data according to security level
- examining and refining standards, policies and procedures pertinent to implementing data security across state government
- identifying how data security relates to privacy and access in Georgia's electronic government (optional)
- developing an implementation plan for data security in state agencies and rolling up the plan to the statewide level, where practical

3.3 Background

The need for secure data cuts encompasses all levels of government. These levels range from national homeland security to security of each state and local agency.

3.3.1 Homeland Security

Homeland security is the top priority of government today; and in this information age, data security is among its top areas. Within this context and environment, the GDADS first identified each of the agency's own security needs. Then, the participants rolled up those needs to the enterprise level.

3.3.2 Enterprise Security

The State of Georgia is faced with numerous upcoming federal and state regulatory statutes that will require special handling of citizen and business data. In examining these requirements, the Georgia Technology Authority must build the security architecture to support them while, at the same time, support e-government to provide trusted services.

The approach of the GDADS was to develop the data security standards that enterprise architecture will incorporate. These standards will impact the areas of policy development and administration, systems and network architecture and operations, and integration of disparate operating systems. They can be used as part of an "open architecture' design, thereby leveraging current technologies while providing the foundation for future information technology (IT) deployments.

Specifically addressing the security of data during transmission, receipt and storage will be the basis for development of a trusted computing environment. Such an environment will support the government's delivery of services to its citizenry.

3.3.3 Agency Information Security Officers

In accordance with the Enterprise Security Policy, Section 4, Organizational Security, each agency will create and maintain an internal information security infrastructure consisting of an information security organization. To implement this policy, each agency shall appoint, designate or hire an Information Security Officer (ISO) to administer its information security program.

Many state agencies have addressed this policy by appointing an ISO. The agency ISOs attend a monthly Georgia Technology Authority open forum – ISO Work Group - where security issues, topics and technologies are discussed and vetted.

Recent topics have included:

- Assessment methodology

- Policy development
- Network accreditation
- Incident response

Technologies that have been introduced include:

- Secure network printing
- Content filtering
- Security management
- Second generation firewalls
- Intrusion detection

Through this forum, members have also been given the opportunity to attend two "boot camps" that provided training in policy development, IT security program development, first response to an incident, firewall and intrusion detection. These boot camps have been part of an overall program to 'seed' the agencies with individuals who can develop and administer an IT security program.

Over the past two years, tremendous progress has been made within the agencies in the implementation of security programs that have commonality in purpose and design. As a state, the agencies have reached a level of maturity and are now preparing to address upcoming federal and state security requirements. This is the point at which the Georgia Digital Academy on Data Security was initiated.

3.4 Pertinent Data Security Legislation and Programs

The following sections describe some of the major legislation and programs that are pertinent to data security at the national and state levels.

3.4.1 Federal Privacy Act of 1974

The Privacy Act of 1974 was the seminal legislation that initiated much of the work on data security. Its importance is in the process and bounds it sets on how private information is handled in the U.S. A copy of the act in its entirety is found in Appendix E to this report.

3.4.2 Georgia Open Records Act

The Georgia Open Records Act established the fundamental protocols for data security in the state. Its importance is in the process and procedures for Georgia's handling of state records. A copy of the act in its entirety is found in Appendix F to this report.

3.4.3 Federal Information Processing Standards (FIPS 199)

Federal Information Processing Standards (FIPS) publications are issued by the National Institute of Standards and Technology. FIPS 199 addresses standards to be used by all Federal agencies to categorize information and information

systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels.

The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

FIPS 199 defines three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The application of these definitions must take place within the context of each organization and the overall national interest. state, local, and tribal governments, as well as private sector organizations comprising the critical infrastructure of the United States, may consider the use of the standards as appropriate.

3.4.4 International Standard Organization (ISO 17799) – Information Technology Code of Practice for Information Security Management

The ISO 17799 standard provides recommendations for information security management to be used by those who are responsible for initiating, implementing, or maintaining security in their organizations. It is intended to provide a common basis for developing organizational security standards and effective security management practices and to provide confidence in inter-organizational dealings. Recommendations from this standard should be selected and used in accordance with applicable laws and regulations.

ISO 17799 is high level, broad in scope, and conceptual in nature. These characteristics allow it to be applied across multiple types of enterprises and applications. The standard is based on the British Standard Institute, Information Security Management standard (BS 7799) and is a comprehensive information security process that covers the selection and management of information security controls. The ISO 17799 document is available for a fee at http://www.iso17799software.com/.

3.4.5 Common Criteria (CC) for Information Technology Security Evaluation

The Common Criteria (CC) is a multipart standard to be used as the basis for evaluation of security properties of IT products and systems. It addresses protection of information from unauthorized disclosure, modification, or loss of use. The categories of protection relating to these three types of security failure are commonly called confidentially, integrity, and availability.

The CC concentrates on threats to information that arise from human activities, whether malicious or otherwise, but may be applicable to some non-human threats as well. It is applicable to IT security measures implemented in hardware, firmware, or software.

The Common Criteria are available at http://csrc.nist.gov/publications/nistpubs/, especially information for NIST Special Publication 800-23 and at http://www.corsec.com/ccc_docu.php.

3.4.6 Federal Bridge

On a national level, the Federal Bridge Certification Authority (FBCA) supports peer-to-peer interoperability among Federal Agency PKI domains. On the state level, this process will be adopted and implemented via a certification authority with oversight directed through GTA and participating agencies in the Data Security User Group. The FBCA will issue a certificate only to those Agency CAs specified by the owning Agency (called "Principal CAs"). The FBCA, or a CA that interoperates with the FBCA, may also issue certificates to individuals who operate the FBCA. The FBCA certificates issued to Agency Principal CAs act as a conduit of trust. The FBCA does not add to and should not subtract from trust relationships existing between the transacting parties. The Federal PKI Policy Authority (FPKIPA) is the governing body over the FBCA that operates under the By-Laws and Operational Procedures/Practices for the FPKIPA (DRAFT). The same procedure will be adopted by the certification authority created for the State of Georgia

At their discretion, agencies may elect to interoperate among themselves without using the FBCA. Those agencies that elect to do so may, nonetheless, employ levels of assurance that mimic those set forth in the FBCA's Certificate Policy (CP). More research is needed to define Object Identifiers (OIDs) that will be used to interoperate via agencies.

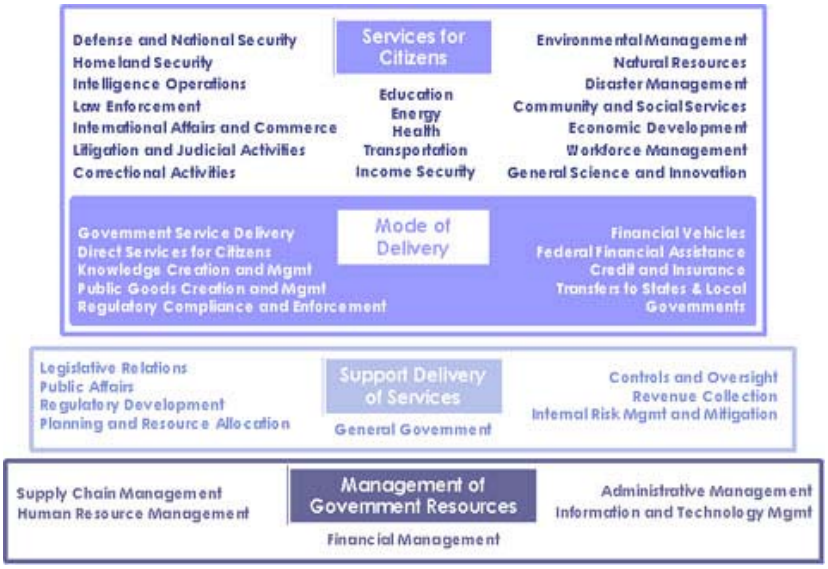
The X.509 Certificate Policy for the FBCA defines five certificate policies for use by the FBCA to facilitate Agency CA interoperability with the FBCA and with other Agency PKI domains. The five policies represent four different assurance levels (Rudimentary, Basic, Medium, and High) for public key digital certificates, plus one assurance level strictly for testing purposes (Test). The word "assurance" used in this CP means how well a Relying Party can be certain of the identity binding between the public key and the individual whose subject name is cited in the certificate. It also reflects how well the Relying Party can be certain that the individual whose subject name is cited in the certificate is controlling the use of the private key that corresponds to the public key in the certificate. This same process has been adopted by Georgia.

U.S. Government Public Key Infrastructure Cross-Certification Methodology and Criteria - This document briefly describes how entities apply for cross-certification and interoperate their PKI with the FBCA. Further work is needed to identify how the Georgia will handle cross-certification.

For more information regarding implementation, updates, etc., please refer to http://csrc.nist.gov/pki/fbca/welcome.html.

3.4.7 Federal Enterprise Architecture

The Federal Enterprise Architecture Program Management Office (FEAPMO) of the Office of Management and Budget (OMB) considers the Federal Enterprise Architecture (FEA) and the Business Reference Model (BRM) as programs that should be built into the annual budget process to repeatedly and consistently improve all aspects of government service delivery. The GDADS participants, Georgia Document Management Association and Georgia Technology Authority have adopted the FEA as a foundation for Georgia's architecture initiatives.



Version 2.0 of the BRM provides an organized, hierarchical construct for describing the day-to-day business operations of the Federal government. It is the first layer of the FEA and the main viewpoint for the analysis of data, service components and technology.

The structure of the BRM consists of a three-tiered hierarchy with Business Areas at the highest level followed by Internal / External Lines of Business and Business Sub-Functions.

The Business Areas separate government operations into the following high-level categories.

- Services for Citizens – defines the purpose of government. It includes the delivery of citizen-focused, public, and collective goods and/or benefits as a service and/or obligation of Georgia's government to the benefit and protection of the nation's general population.

- Mode of Delivery – defines the mechanisms used by government to achieve its purpose. It includes Financial Vehicles and Direct/Indirect government delivery.
- Support Delivery of Services – defines the support functions necessary to conduct government operations; i.e., critical policy, programmatic and managerial tasks.
- Management of Government Resources – defines the resource management functions that support all areas of government's business; i.e., back-office support activities.

The Business Areas are comprised of 39 lines of business categorized as either External or Internal. The "external" lines of business consist of 19 areas identified in the Services for Citizens. The "internal" lines of business consist of 20 areas described as support functions the government must conduct to effectively deliver services to citizens. Each line of business is a collection of 153 sub-functions that represent the lowest level of granularity in the BRM.

3.4.7.1 Benefits of the BRM – For the Citizen

The true driver behind the FEA effort is the need to improve the government's delivery of services to the public. The stove-piped, agency-centric processes that have previously characterized government must be replaced with citizen-centric processes. The same driver is key to Georgia agencies' adoption of this framework.

3.4.7.2 Benefits of the BRM - For Federal Agencies

The BRM "vision" into the federal architecture gives each agency a collection of new capabilities for defining and implementing their own target environments. Agencies will now be able to:

- Adopt this framework which will put Georgia in line with the Federal Government, thereby allowing them to save time and money by leveraging reusable business processes, data, and IT components of other agencies.
- Leverage FEA work products as a catalyst for agency-specific EA efforts.

- Ensure that proposed investments are not duplicative with other agencies' prior to developing business cases and submitting them to OMB.
- Suggest modifications to the BRM to ensure that future versions accurately portray the business of the U.S. government, including the roles that specific agencies play.

3.4.7.3 Benefits of the BRM - For Legislatures

Application of the Federal Enterprise Architecture will yield a wealth of information on Federal and state business lines, programs and capital investments and their performance. This information will be made available to the legislature as it considers the authorization and appropriation of funding for state programs, and as it fulfills its oversight responsibilities to ensure that state funds are appropriately spent.

For more information regarding implementation, updates, etc., please refer to http://www.feapmo.gov/.

3.5 XML and XML Schema

Moving data securely among agencies and other organizations is a technical challenge. To meet this challenge, the GDADS participants investigated techniques using XML and XML schema. We found that many existing XML schema are promising for aiding Georgia's quest for data security.

3.6 GTA Policies, Standards, and Guidelines

The GTA has established a process for developing and implementing policies, standards, policies and guidelines for IT statewide. With respect to data security, the user group resulting from this Digital Academy will recommend standards to the GTA. Further information is contained in Appendix A.

3.7 Major Issues in Data Security

Data is the representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. An overwhelming amount of data today is created, gathered, stored, accessed, transmitted, and disposed of electronically; and the data used by Georgia is no exception. In light of this fact, the security of this data is critical to the proper operations of the state's agencies.

Data has three commonly recognized attributes: confidentiality, integrity and availability:

- **Confidentiality** may be defined as the protection of sensitive information from unauthorized disclosure and sensitive facilities from physical, technical or electronic penetration or exploitation. The GDADS' work included definition of the levels of confidentiality applicable to the state's data and discussion of the resulting levels of protection required to be applied to these different levels of confidentiality when the data is created, stored, transmitted, or disposed.

- **Integrity** may be defined as the condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. Once data has been classified for confidentiality, the required level of integrity for that data should be

determined and the appropriate methods to ensure data integrity defined and instituted. Establishment and implementation of best practices will allow state data to be trusted by the citizenry, businesses and other governmental agencies. The state's agencies may take advantage of such technologies as PKI in order to address the integrity issue.

- **Availability** refers to the ability to obtain or access data when necessary. The increasing dependence of the state on networked applications, the Internet, Intranets, etc., require the creation of an environment to provide a high level of data availability.

Threats to data security may be posed by a variety of "weaknesses" - technology, configuration, policy, and human are some of the more prominent ones. For example, TCP/IP was designed as an open standard with no thought of security. Configuration weaknesses include misconfiguration of hardware and software, which creates security problems. Also, security policies may be poorly defined or improperly implemented and managed. And, of course, human error is considered by many to be the largest threat to data security.

The focus of the GDADS was to accomplish (via collaboration and education of state agencies) the identification and standardization of best practices for data security and develop plans and solutions to meet the business requirements for data security in state agencies.

3.8 Related Issues in Data Security

Privacy refers to an individual's ability to control how his or her personally identifiable information (e.g., social security number, financial and health data) is used and communicated. Lack of control over such information may lead to identity theft, a crime in which one person masquerades under the identity of another. Personal data stored by the state's agencies must be protected against unauthorized access in order to prevent exploitation.

4. METHODS AND PROCEDURES

The Georgia Digital Academy on Data Security (GDADS) was designed to ensure that participants could receive maximum benefit from their attendance while, at the same time, being able to continue to fulfill their regular job responsibilities. An overview of the structure of the sessions follows:

1. Initial session on data mapping - June 17 and 24 and July 8, 2003

2. Break and attendance at statewide conference on Privacy and Access Issues in Georgia E-Government - July 16, 17, 23, 24, 30, and 31.

3. Session on data categorization - August 12, 19, and 26, 2003

4. Session on technical standards in data security - September 23 and 30 and October 7

5. Final session on development of a strategic implementation plan for data security - November 4, 11, and 18

Participants invested a great deal of effort in the academy and can expect to receive maximum benefits for their investment. To meet these expectations, the academy used a variety of techniques developed especially for adult instruction and collaborative problem solving. These techniques were implemented in a setting free from the distractions of today's busy offices. The following sections describe some of the prominent features of the academy.

4.1 Facilitated, Interactive Sessions

People often learn best when interacting with each other and actively practicing new skills. The academy included facilitated learning sessions structured around an ongoing group activity—planning and designing for data security—and short, individual homework exercises.

Although state agencies have widely varying roles and responsibilities, they face many of the same challenges in using IT to meet their business needs. Participants worked in a collaborative way to identify solutions they can all share. They helped set the direction, standards and other requirements for implementing data security and related technical functions in state government.

4.2 Continuous Improvement and Web-based Research

Information Technology standards and best practices are changing rapidly. To help participants keep up with these changes, the academy emphasized continuous improvement—that is, *learning to learn*. Participants also explored the best sources on the Web and elsewhere for the latest information about IT standards and practices.

4.3 An Ongoing Group Activity: Planning for Data Security

State agencies taking part in the academy were expected to be actively planning the implementation of data security. Beginning with data mapping and data categorization for each agency, participants shared and reviewed each other's situations and requirements and worked them into technical standards and an implementation plan for data security. The plans represented the needs of the participating agencies as inclusively as possible. Academy facilitators guided participants through the data mapping, categorization, technical standardization, and planning.

4.4 Subject Matter Experts (SMEs)

The academy hosted select experts and implementers of data security. Participants met and worked with qualified SMEs and consultants, heard firsthand accounts from organizations with experience in implementing large and complex data security projects, and examined the latest techniques and designs utilizing data security. They included:

- Kevin Baker, Georgia Technology Authority
- Moses Miles, Georgia Technology Authority
- Richard Halstead-Nussloch, Southern Polytechnic State University
- Doug Nassar, Logical Choice Technologies
- Andrew Taylor, Secretary of State/Georgia Archives
- Amelia Winstead, Secretary of State/Georgia Archives

4.5 Division into Two Groups of Interest

The number and the diversity of participants suggested division into two breakout groups for active discussion of data mapping and access classification. Following up on a suggestion from the floor, the participants from the courts and law enforcement agencies formed a breakout group and adopted "The Justice League" as their name. The remaining agencies became known, eventually, as the "Business League."

The Justice League was composed of the following agencies:

- Administrative Office of the Courts
- Georgia State Patrol
- Georgia Bureau of Investigation
- Department of Juvenile Justice,
- Department of Corrections
- State Board of Pardons and Paroles

The Business League was composed of the following agencies:

- Department of Community Affairs

- Department of Banking and Finance
- Department of Transportation
- Georgia Student Finance Commission
- Department of Administrative Services

The academy staff of the Georgia Technology Authority, Department of Audits, Archives Division of the Office of the Secretary of State and Southern Polytechnic State University divided their attention between the Justice League and the Business League.

5. RESULTS AND DISCUSSION

5.1 Findings

5.1.1 Data Mapping

All agencies worked on developing a data map, a large and complex task. To reduce this task's size and complexity, a process was developed and implemented on a trial basis. This process proved successful in a) producing meaningful data maps for the agencies and b) providing the ability for implementation of it across a wide spectrum of agencies. Evidence of the success of this approach is indicated by the choice of data mapping as the initial area for data security standardization.

The ability of the process to be implemented statewide is reflected in the recommended GTA standard found in Appendix A.

The recommended process is described in the advice section of the standard found in Appendix B.

A sample data map is found in Appendix B. Within the scope of the academy session, it shows the major categories of applications within the Department of Administrative Services (DOAS).

5.1.2 Data Categorization

All agencies worked on developing a set of data categories and implemented the categorization on their data maps. The following process proved successful in doing so:

1) Read FIPS 199 -- 12 Pages - 1 hour

http://csrc.nist.gov/publications/drafts/FIPS-PUB-199-ipd.pdf

2) Examine the critical business processes and operations in your agency. Review your agency's IT strategic plan. - 2 hours

3) Talk to the data owners in your agency, discussing the data security aspects of a) platforms and b) users. - 2 hours

4) Develop for your agency a data map and an access matrix. - 1 hour

5) Review the map and matrix with your agency's strategic planner. - 1 hour

6) Review the possibilities for using XML in mapping your agency's data. Look for using it as a description language for your data mapping and as a path to

common definitions. Look for existing XML schema that can be used in your agency. - 1 to 4 hours

Further information is contained in Appendix A which covers the recommended standard. The GDADS recommends that implementation plans for data security be the subject of a future workshop.

5.1.3 Privacy and Access

The Archives Division of the Office of the Secretary of State sought and obtained a $40,625 grant from National Historic Publications and Records Commission (NHPRC) to partner with Southern Polytechnic State University (SPSU) to provide statewide education on privacy/access issues and e-government for Georgia's state and local government as well as produce a white paper on this topic.

The "Privacy and Access Issues in Georgia E-Government Conference" was held on Wednesdays and Thursdays beginning July 16 through July 31 from approximately 9:00 a.m. to 3:30 p.m. To encourage attendance, the dates were spread over three weeks rather than ask attendees to be absent from work at the end of the fiscal year for six straight days. Because it seemed to present the most difficulty, the conference focused on citizen data (also known as digital identity) as a major topic.

Each day was organized so that a speaker gave a 1 to 2 hour presentation, followed by a facilitated question/discussion session. The sessions were paired each day so that a speaker discussed the national perspective on an issue and was followed by a second speaker discussed the issue from a statewide or agency perspective. An agenda for the conference is found in Appendix H.

The first day of the conference was spent orienting the participants to the conference topic. Dr. Paul M. A. Baker of the Georgia Centers for Advanced Telecommunications Technology and Mr. Richard Keck of the Troutman Sanders law firm discussed “Policy Perspectives on Government Use of Citizen Data: Balancing the Need for Privacy.” The remaining sessions addressed the following specific questions:

- Should there be a classification or categorization scheme for private information? If yes, what elements need to be considered in the development of this scheme?
- Is information regarding certain individuals in need of greater security than others? Is all information created equal or is some "more equal" than others?
- If we are able to define specifically what is to be kept private for government, how do we identify that information sufficiently to enable technology to protect it?

The speakers and topics for the sessions follow:

- Paula Arcioni, New Jersey, Office of E-Government Services and Odysseus Marcopolus, New Jersey, Office of E-Government Services - "Let's Not Reinvent the Wheel"

- Kathryn Allen, Georgia Office of Attorney General – "Laws, Rules, and Regulations Impacting Georgia E-Government"

- Emily Frye, Georgia Mason University – "Digital Identity: A Discussion"

- Dr. Charles Dollar, Dollar Consulting – "Planning for the Long-Term: When Digital Identity and E-Records Must be Maintained"

- Andrew S. Taylor, Georgia Archives – "Lifecycle Management of Georgia's E-Records"

Following the presentations were two days of working group meetings to outline a set of implementation policies/guidelines for use by Georgia government. Further work on the implementation guidelines took place via meetings, the project website and email. The Georgia Technology Authority worked with the Archives and SPSU to assist in the development and approval of privacy policies for all of state government. For local governments (both county and municipalities), policy recommendations and implementation guidance will be presented in future workshops.

The last day was spent wrapping up the conference. Dr. Richard Halstead-Nussloch and Amelia Winstead, Georgia Archives, reviewed the conference topics and led the attendees in drafting the outline of the white paper.

5.2 Significance of Findings

5.2.1 Data Mapping produced the methodology by which agencies should identify and prioritize systems, applications and data that are critical to support business functions and strategic goals. A matrix was developed that will assist any agency in identifying key elements that support business functions. Using this matrix, the agencies can prioritize and direct resources to meet compliance issues for regulatory statutes involving the storage, transmission and authentication of data.

5.2.2 Data Categorization was perhaps the most difficult segment to produce. Using federal guidelines found within FIPS 199, the academy examined the various types of data produced and created categories by which it could apply FIPS 199. The resulting work will have a major impact on the administrative policies, operational procedures, and IT architecture. These categories and associated technical standards for protection establish the degrees of value for an

agency's data, thereby allowing the agency to direct policies, technology and operations towards standards-based compliance.

5.2.2.1 Technical Standards for data security are broad based and are mapped back to known federal requirements. Anticipated requirements were considered and incorporated.

5.2.2.2 Implementation Plans show that the process will take at least three years to begin. This was due to the current budget cycle in conjunction with needed adjustments to individual agency strategic plans. Legacy systems and future IT deployments may be impacted as well.

5.2.3 Privacy and Access Conference played an important role in defining the hierarchy of record/documents whereby data first becomes information and then a record. This provided the needed guidance to separate the technological definitions from constitutional definitions although the 'bits and bytes' are the same. Having this guidance was invaluable in the creation the of data categories.

5.3 Implications of Findings

The work of the Georgia Digital Academy on Data Security will bring about substantial implications to government's handling of data, information and official records. Having established certain value or worth for data, there are a number of issues to be addressed. Issues on privacy, accessibility, security and assurance will come to the forefront for policy, systems and network architecture, data access and assurance. Levels of trust can now be appropriately implemented through subsequent development of policies, procedures and the deployment of applicable technologies to meet compliance with regulatory statutes.

"Trust level" and "Assurance level" are terms to that can be interchanged within the context of a security framework regarding the enterprise. The reference for the development of the trust levels were based upon federal documentation (Common Criteria) used for financial systems. It was viewed as being the most stringent in security terms but required supplementation by other documents (National Institute of Standards in Technology) for more granular explanation and standards. Leveraging these federal guidelines in the categorization of the state's data ensured continuity in interfacing state systems and applications with federal partners. Reaching the goal of establishing a trusted computing environment may not be measured until there is federal accreditation.

Strategically thinking, this effort establishes the foundation for the development of an IT infrastructure that will support a trusted computing environment to foster government efficiency and enhance secured services for businesses and citizens through technology interfaces. The categorization effort developed communities of interest among the participating state agencies. Among the benefits derived from these communities of interest were the discovery of common processes, data, applications and realization of IT infrastructure of

individual agencies. In addition, the development of an implementation template allowed the agencies to better focus strategic planning thereby prioritizing affected IT programs and projects. In totality, the GDADS addressed the essence of securing data by which all other elements of information technology, policy and procedures can be addressed.

5.4 Recommendations

The primary output of the Georgia Digital Academy on Data Security is the development of a series of recommendations to be used by agencies, the Georgia Technology Authority, and the State of Georgia in the initiation of guidelines for data security planning and implementation.

5.4.1 For Agencies

Develop and implement an agency-specific data security plan.

5.4.2 For the Georgia Technology Authority and State of Georgia

- Continue to provide a forum for state agencies to collaborate and develop solutions to common issues associated with data security.
- Develop and implement an enterprise information security standard for data categorization based on the recommendations contained in the advice document.
- Support the roll-up of agency data categorization implementation plans to the state enterprise level.
- Partner with agencies to facilitate a data security work group to develop a long- term strategy and implementation plan that addresses the needs of the state and agency business programs.
- Develop and implement state enterprise data security standards to support technology and infrastructure requirements that are in line with the Federal Enterprise Architecture.

6. REFERENCES AND BIBLIOGRAPHY

1. **E-Government Act of 2002 (Public Law 107-347)** - http://stats.bls.gov/opub/cwc/cm20030220yb02p1.htm

2. **Federal Information Security Management Act of 2002** - http://www.fedcirc.gov/library/legislation/FISMA.html

3. **National Institute of Standards and Technology** - http://www.nist.gov/

4. **GTA Standardization Process** – (Internal Policies) - http://gtainsider.gagta.com/policiesprocedures/policiesprocedures.html

   (Enterprise Policies) – http://gta.georgia.gov/00/channel_modifieddate/0,2096,1070969_6947051,00.html

5. **Privacy Act of 1974** - http://www.usdoj.gov/foia/privstat.htm

6. **Georgia Open Records Act** – http://www.sos.state.ga.us/Archives/rms/ora.html

7. **Federal Information Processing Standards (FIPS) 199** - http://csrc.nist.gov/publications/fips/index.html

8. **ISO 17799** - http://www.iso17799software.com/

9. **Common Criteria for Information Technology Evaluation** - http://csrc.nist.gov/publications/nistpubs/, especially information for NIST Special Publication 800-23 and at http://www.corsec.com/ccc_docu.php

10. **Federal Bridge Certification Authority** - http://csrc.nist.gov/pki/fbca/welcome.html

11. **Federal PKI Policy Authority (FPKIPA)** - http://www.fts.gsa.gov/netconference/lasvegas44/sld010.htm

12. **X.509 Certificate Policy for the FBCA** - http://www.pubklaw.com/ecomm/fbcacp03122001.pdf

Formatted: Italian (Italy)

13. **U.S. Government Public Key Infrastructure Cross-Certification Methodology and Criteria** - http://csrc.nist.gov/pki/fbca/welcome.html

14. **Federal Enterprise Architecture Program Management Office (FEAPMO)** - http://www.feapmo.gov/

15. **National Historic Publications and Records Commission** http://www.nagara.org/clearinghouse/winter_97/nhprc.html

APPENDIX A

Data Categorization Standard

State of Georgia

Georgia Digital Academy - Data Security

Security Categorization of Agency Information and Information Systems

Document Version: Initial Draft 100603

Document Revision History			
Rev	**Description of Change**	**Author(s)**	**Effective Date**
0	First Draft	Sherman Harris, DOAS Maris Wynn, DCA Bill Wyatt, Dept. of Audits	09/30/03
1	Update Review Comments	Sherman Harris	10/03/03
2	Update Process Steps	Maris Wynn	10/06/03
3	Update Process Steps; Create Advice Document	Sherman Harris, Maris Wynn, Bill Wyatt	11/04/03
4	Finalize Standard and Advice Documents	GDADS	11/05/03 and 11/12/03

Reference Documents	
Document Number	**Document Title**
NIST FIPS-PUB-199	Initial Public Draft - Standards for Security Categorization of Federal Information and Information Systems
	Common Criteria/ISO 15408
	Privacy Act of 1974

1. OVERVIEW

Georgia state agencies store a large amount of data that requires various security levels. There is currently no overall listing of the data stored, so that data may be shared among different agencies and in some cases the same information may be collected separately by several agencies. Without an awareness of the data available and the security policies used by each agency, information considered by one agency to be high-security could be made available by another agency at a lower security level. In some cases, agency users may not be aware of security restrictions on data, such as Federal or state law.

This proposed standard provides a method for agencies to use in collecting and categorizing their data so that data common to several agencies can be recognized and assigned the same risk level. The risk levels assigned may be determined by the agencies involved or may be set based on Federal or state laws and regulations, thus ensuring compliance with legal requirements. Agencies can use data mapping as an internal inventory to document databases used and the information stored. Data mapping can also highlight information collected and stored separately by several agencies. Such information might a candidate for consolidation, collected in one place and then shared among various agencies.

2. SCOPE

The goal of this document is to define and document a process that will allow state agencies to consistently perform data categorization as part of an overall data security implementation plan. As part of its charter, the Georgia Digital Academy on Data Security is tasked with developing and recommending Data Security Standards that will protect the confidentiality, integrity, and availability of agency data assets. The proposed standards will also align the agencies with the Federal Enterprise Architecture Framework that will be the basis for information and data sharing between Federal and state governments.

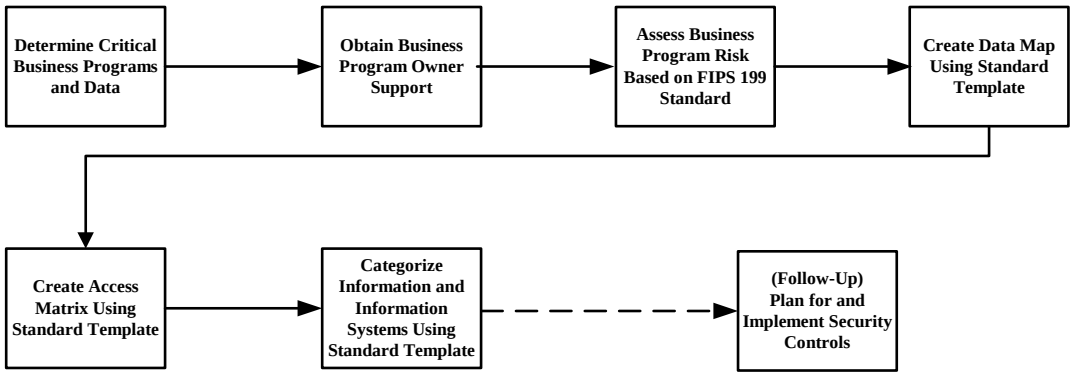
The building block of this architectural framework is the consistent Data Mapping and Categorization of agency data assets based on the Federal Information Processing Standard (FIPS) 199.

3. SECURITY CATEGORIZATION PROCESS

The security categorization process as referenced in Figure 1 is based on the FIPS 199 Federal Information Processing standard. It establishes three potential levels of risk (low, medium, and high) for each of the stated security objectives (confidentiality, integrity, and availability) relevant to securing agency information and information systems. The levels of risk consider both impact and threat, but are more heavily weighted toward impact. The impact is based on the potential magnitude of harm that the loss of confidentiality, integrity, or

availability would have on agency operations and business programs (including mission, functions, image, or reputation), agency assets, or individual privacy.

Figure 1: Categorization of Information and Information Systems Process Flow.



Step 1: Determine Critical Business Programs and Data

Business owners and agency management should be consulted to identify critical business programs and data. Their input is critical in determining risk levels based on impact and threat. They should also be consulted before implementing controls to mitigate risk, to ensure that selected controls do not negatively impact business operations.

Critical business programs include any programs whose functioning is essential to the mission of the agency.

Step 2: Obtain Business Program Owner Support

This is one of the most critical steps in implementing the security categorization process, as business owners have the final knowledge of and control over their data. Business owners should have a clear understanding of the need for performing security categorization, and how it will benefit their programs.

Step 3: Create Data Map Using Standard Template

The data map lists the critical program databases maintained by the agency. It covers three areas:

- What is the name and function of the database system?

- Who owns the data, who uses the data, and who maintains the database system?
- How and where is the data stored?

A thorough and accurate data map is essential for security categorization. It may also initiate further discussion with business owners.

Step 4: Assess Business Program Risk Based on FIPS 199 Standard

The FIPS 199 Standard recommends that each data system be evaluated for risk in three areas: confidentiality, integrity, and access. Risk levels should be classified as High, Medium, or Low. If data records at different risk levels are stored in the same system, the system should be given the highest applicable risk level.

The Advice document includes a table of risk levels that have been determined for major data system types. It also includes guidelines and a template for completing a more detailed categorization and rolling up the results to the Data Access Matrix. This step is not required but is highly recommended.

Step 5: Create Access Matrix Using Standard Template

The Data Access Matrix is used to determine the appropriate levels of access for each system listed in the data map. The Advice Document defines these trust levels.

These trust levels will determine the user authentications to your data systems.

Follow-Up: Plan for and Implement Security Controls

This categorization process will result in a data map and a categorization of your data systems and elements that you can use to determine what, if any, additional security controls and procedures may need to be put in place. See applicable standards for this process.

6. SUMMARY

The State of Georgia has defined a standard that should be used to map and categorize all of the data/resources within your agency. The intent of implementing this standard is to enable all of the state agencies to readily know what type of data they are storing, how the data should be accessed, and at what level of sensitivity the data should be defined. Establishing and implementing this standard will be the first steps toward allowing agencies to effectively and securely communicate with other state, local, and federal agencies.

The documents within this standard are considered the template in which agencies will define their information. The consistency in which agencies perform this process is essential to the overall effectiveness of this standard. The Data Map should be used to, in essence, inventory the data you own. The Data Access Matrix will be used to directly categorize your information to the appropriate security level. Along with these two templates, we have also provided a template/process in which agencies can define the more detailed information about their data. This template includes elements such as tables, fields, level of sensitivity, and a direct relationship back to the data mapping document. Keep in mind that the third document is not required, but is helpful in organizing as you attempt to define the level of sensitivity within the data.

APPENDIX B

Data Categorization Advice Document

State of Georgia

Georgia Digital Academy - Data Security

Security Categorization of Agency Information and Information Systems

Advice Document

Document Version: Initial Draft 101003

Definitions:

Trust
A level of protection in the transmission and authentication required to complete transactions.

Risk Levels
In accordance with FIPS-199, we have adopted risk levels based on the following associated level of risk. The highest risk level for a data category determines the required minimum level of trust.

Table 1 (copied from FIPS Publication 199) summarizes the potential impact definitions for each security objective in FIPS 199—confidentiality, integrity, and availability.

Security Objective	Potential Impact: Low	Potential Impact: Moderate	Potential Impact: High
Confidentiality Preserving authorized restrictions on informaiton access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., Sec. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., Sec. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., Sec. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Data Map

- The data map lists critical program databases maintained by the agency. It is essentially an inventory of agency databases. The Data Map Template in

Table 1 is the standard for used to record this inventory. The columns in the form are described below.

- *Agency*: Your agency name.
- *System Function*: General type of database or database system: for example, "PeopleSoft" or "Risk Management".
- *Sub System*: Specific system within the overall system function (may not be necessary in all cases): for example, "Workers' Comp/Claims" (part of Risk Management)", or "Vendor Registration" (part of State Purchasing).
- *Owner*: Who has the ultimate authority over this data? This can be listed as user groups or categories rather than individual staff – "the HR Department", for example.
- *Custodian*: Who manages the hardware and software used to store the data? This would include server administrators, DBAs, and database or web developers. Again, this can include staff categories instead of individual users.
- *Users*: Who works with – adds, updates, deletes, or views – all or part of the data in this system? This can be by type of user rather than specific individual: for instance, "general public" or "users of the GTA portal".
- *Hardware Platform*: Mainframe, open system, or Intel-based.
- *Operating System*: The operating system of the server upon which the database is stored.
- *DBMS*: The database management system, e.g., SQL Server, Access or Oracle. For proprietary systems, include the name of the vendor also, e.g., PeopleSoft/Oracle.
- *Data Category*: Table 3 lists the most common inter-agency categories of data. If your information does not fall into one of these categories (that is, it is Agency-Specific), specify a category that you feel is most appropriate.

Template Descriptions:

Data Access Matrix

- The Data Access Matrix form in Table 2 is used to determine the appropriate levels of access for each system listed in the data map. The Risk and Assurance levels are the highest levels appropriate for the entire system – for example, if some system elements are high-risk while others are low-risk, the system as a whole is given a high risk level
-
  - *Agency*: Your agency name.
  - *System Function*: General type of database or database system (see Data Map listing).
  - *Sub System*: Specific system within the overall system function (see Data Map listing).
  - *Internal Access*: Users and groups within the agency who have access (view or edit) to the data.
  - *External Access*: Users and groups in other agencies or part of the general public who have access (view or edit) to the data.

- *Risk Level*: defined above.
- *Trust Level*: defined above.

Data Categories

The Data Categories listed in Table 3 are the most common types of inter-agency data. When possible, assign your data to one of these categories – this will help ensure that similar kinds of information are treated alike by all agencies. Some examples are given below for each category.

- *Criminal Justice*:
    - Release Decision info
    - Law enforcement info
    - Investigations info
    - All case info
    - Criminal history record
    - Release decision data
- *Financial*:
    - Court reporting
    - Contracts
    - Purchasing info
    - Procurement info
    - Budget info
    - Check processing
    - Construction estimates info
    - Grants and loans financial info
    - Financial assistance info
    - Collections info
    - Fees
- *Infrastructure*:
    - <u>IT</u>
        - Migration to AD
        - Outstanding problems, especially security problems
        - Internal File system for LAN
        - Email
        - Firewalls
    - <u>Physical</u>
        - Bridge construction diagrams
        - Blueprints
        - Technical specifications
        - Evacuation plans
- *Medical*:
    - Treatment info
    - Counseling info
    - HIPAA info
    - Employee medical

- *Administrative*:
    - Fleet maintenance information
    - Inventory and asset management
    - Surplus administration
    - Phone assignments
    - Permits
    - Contact information
    - Garage information
    - Firehouse information
    - Construction delays
    - Space management
    - Supplier information
- *Human Resources*:
    - Employee personal information
    - Payroll information
    - Benefits records
    - Listings of job codes and organization codes
    - Position information
- *Legal*:
    - Property damage claims
    - Lawsuits, Malpractice, Workers Comp
    - Civil case records
    - Contract tracking
- *Education*:
    - ADAP
    - Student records
    - Research data
- *Agency-Specific*: Data that does not fall into one of the general inter-agency categories listed above. When possible, try to group your agency-specific data, so that you have several systems in each agency-specific category rather than assigning a new category to each system. Examples include:
    - Local government contacts
    - General information on grants and loans
    - Service directories
    - Disposition of cases
    - Statistics
    - Public information
    - Agency information

Data Categorization Template

The Data Categorization Template (Table 4) is not required, but you may find it useful in creating the Data Access Matrix.

- *System/Database*: Maps to System Function and SubSystem

- *Data Record*: Individual element within the subsystem (may also be at the subsystem level.
- *Confidentiality*: Assigned from FIPS-199 criteria.
- *Integrity*: Assigned from FIPS-199 criteria.
- *Availability*: Assigned from FIPS-199 criteria.
- *Comments*: Any information about special issues with or requirements for managing this data.

Categorization Templates

Table 1: Data Map Template

Agency	System Function	Sub System	Owner	Custodian	Users	Hardware Platform	Operating System	DBMS	Data Category *

** See Table 3 for Data Category list.*

Table 2: Access Matrix Template

Agency	System Function	Sub System	Internal Access (Groups)	External Access (Groups)	Risk Level *	Trust Level

** Risk Levels are defined in the FIPS 199 standard.*

Table 3: Data Category Risk Levels

Data Category *	Risk Level (Low, Medium, High)	Notes
Criminal Justice	**Medium**	
Financial	**Medium**	
Infrastructure	**Medium**	
Medical	**Medium**	
Administrative	**Medium**	
Human Resources	**Medium**	
Legal	**Medium**	
Education	**Low**	
Agency-Specific	**Variable**	Likely to include specific areas of High Trust Level
Personal Data Set	**Variable**	From Privacy Act of 1974; Assumes redaction will be completed

***** *See above for definitions*

Note: Although no high trust levels were identified, that does not preclude individual applications at high within the categories.

Table 4: Data Categorization Template (can be used to create the Data Access Matrix)

System/ Database	Data Record	Confidentiality *(Low, Medium, High)*	Integrity *(Low, Medium, High)*	Availability *(Low, Medium, High)*	Comments

This section shows an example of a completed Data Map and Access Matrix for the PeopleSoft HR system.

Example Data Map Template

Agency	System Function	Sub System	Owner	Custodian	Users	Hardware Platform	Operating System	DBMS	Data Category *
DOAS	PeopleSoft	HR	HR	IT Department	HR .	Mainframe	OS/400	PeopleSoft/ Oracle	Human Resources

Example Access Matrix Template

Agency	System Function	Sub System	Internal Access (Groups)	External Access (Groups)	Risk Level *	Trust Level
DOAS	PeopleSoft	HR	HR	none	High	

Example Data Categorization Template (used to create the Data Access Matrix)

System/ Database	Data Record	Confidentiality *(Low, Medium, High)*	Integrity *(Low, Medium, High)*	Availability *(Low, Medium, High)*	Comments
PeopleSoft HR	Employee record	H	H	M	
PeopleSoft HR	Position record	L	H	M	
PeopleSoft HR	Job Codes	L	H	M	
PeopleSoft HR	Employee Benefits records	H	H	M	

Table of Required Security Levels by Data Category

Data Category	Possible XML Schema	Trust Level	Storage Encryption Rate	Transmission Encryption Rate	Authentication Level
Legal	Justice XML	Medium	0	128K	2
Criminal Justice	Justice XML	Medium	0	128K	2
Human Resources	TBD	Medium	0	128K	2
Admin	TBD	Medium	0	128K	2
Medical	TBD	Medium	128K	128K	2
Education	EDXML ***	Low	0	128K***	1
Financial	TBD	Medium	128K***	128K***	2
Infra-Structure for IT	XML.20	Medium	0	128K***	2
Infra-Structure for physical	XML.20	Medium	0	128K	2
Agency-Specific	TBD	Variable**	Variable**	N/A	N/A
Personal Data Set	TBD	TBD	TBD	TBD	TBD

* from Privacy Act of 1974
* assumes automatic redaction
** likely to include specific areas of High Trust Level

Although no high trust levels were identified, that does not preclude individual applications at high within the categories.

APPENDIX C

Glossary

1. **Authentication** – Process by which assurance of identity can be verified.

2. **Availability -** Ability to obtain or access data when necessary.

3. **Common Criteria - Common Criteria (CC) for Information Technology -** A multipart standard to be used as the basis for evaluation of security properties of IT products and systems. It addresses protection of information from unauthorized disclosure, modification, or loss of use. The categories of protection relating to these three types of security failure are commonly called confidentially, integrity, and availability.

4. **Confidentiality -** Defined as the protection of sensitive information from unauthorized disclosure and sensitive facilities from physical, technical or electronic penetration or exploitation.

5. **Data -** Distinct pieces of information, usually formatted in a special way.

6. **Data Access Matrix -** The Data Access Matrix form in Table 2 is used to determine the appropriate levels of access for each system listed in the data map.

7. **Data Category –** Data that has been grouped because of similarity in business, functional or regulatory requirements.

8. **Data Manager –** Technical entity who has the responsibility to organize, store, transmit and ensure integrity of data.

9. **Data Map -** The data map lists critical program databases maintained by the agency. It is essentially an inventory of agency databases.

10. **Data Owner –** Functional business entity responsible for the creation, collection of data to support a business requirement.

11. **E-Government Act of 2002 -** The E-Government Act of 2002 (Public Law 107-347), passed by the one hundred and seventh Congress and signed into law by the President in December 2002, recognized the importance of information security standards to the economic and national security interests of the United States.

12. **External Access -** Users and groups in other agencies or part of the general public who have access (view or edit) to the data.

13. **Federal Bridge -** On a national level, the Federal Bridge Certification Authority (FBCA) supports peer-to-peer interoperability among Federal Agency PKI domains.

14. **Federal Enterprise Architecture Framework –** Business and performance-based framework to support cross-agency collaboration, transformation, and government-wide improvement.

15. **Federal Information Security Management Act of 2002 -** Tasked the National Institute of Standards and Technology with developing standards to be used by all Federal agencies to categorize all information and information systems collected or maintained by each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels.

16. **The Privacy Act of 1974 -** Seminal legislation that initiated much of the work on data security. Its importance is in the process and bounds it sets on how private information is handled in the U.S.

17. **FERPA** (**Family Educational Rights and Privacy Act**) - A Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

18. **Federal Information Processing Standards (FIPS) 199 -** Defines three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability).

19. **Information –** The compilation of data, data sets used to support a business requirement.

20. **Integrity -** The condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

21. **Internal Access -** Users and groups within the agency who have access (view or edit) to the data.

22. **ISO 17799 –** A standard that provides recommendations for information security management to be used by those who are responsible for initiating, implementing, or maintaining security in their organizations. It

is intended to provide a common basis for developing organizational security standards and effective security management practices and to provide confidence in inter-organizational dealings.

23. **Non-repudiation -** In reference to digital security, *non-repudiation* means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

24. **PKI -** Short for *public key infrastructure*, a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction. PKIs are currently evolving and there is no single PKI nor even a single agreed-upon standard for setting up a PKI. However, nearly everyone agrees that reliable PKIs are necessary before electronic commerce can become widespread. A PKI is also called a *trust hierarchy*.

25. **Privacy -** Refers to an individual's ability to control how his or her personally identifiable information (e.g., social security number, financial and health data) is used and communicated.

26. **Record -** Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

27. **Sensitive Data –** Data that in of itself or in aggregate form that may be inadvertently or intentionally disclose would expose the subject and organization to risk or harm.

28. **Standards -** A definition or format that has been approved by a recognized standards organization or is accepted as a de facto standard by the industry. Standards exist for programming languages, operating systems, data formats, communications protocols, and electrical interfaces.

29. **System Function -** General type of database or database system.

30. **TCP/IP -** Abbreviation of *Transmission Control Protocol*, and pronounced as separate letters. TCP is one of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data.

TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

31. **Trust -** A level of protection in the transmission and authentication required to complete transactions.

32. **XML -** Short for *Extensible Markup Language*, a specification developed by the W3C. XML is a pared-down version of SGML, designed especially for Web documents. It allows designers to create their own customized tags, enabling the definition, transmission, validation, and interpretation of data between applications and between organizations.

33. **XML Schema -** Short for *XML Schema Definition*, a way to describe and validate data in an XML environment. (A *schema* is a model for describing the structure of information.) XSD is a recommendation of the W3C.

APPENDIX D

Distribution List

- Account Managers
- Agency CIOs
- Agency Heads
- CIO Council
- Data Security User Group
- GDADS Participants
- Governor's Office
- Homeland Security

APPENDIX E

THE PRIVACY ACT OF 1974[1]

5 U.S.C. § 552a

As Amended

§ 552a. Records maintained on individuals

(a) Definitions

For purposes of this section--

(1) the term "agency" means agency as defined in section 552(f) of this title;

(2) the term "individual" means a citizen of the United States or an alien lawfully admitted for permanent residence;

(3) the term "maintain" includes maintain, collect, use or disseminate;

(4) the term "record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph;

(5) the term "system of records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual;

(6) the term "statistical record" means a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of Title 13;

(7) the term "routine use" means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected;

(8) the term "matching program"--

[1] From http://www.usdoj.gov/foia/privstat.htm

(A) means any computerized comparison of--
(i) two or more automated systems of records or a system of records with non-Federal records for the purpose of--
(I) establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or

(II) recouping payments or delinquent debts under such Federal benefit programs, or

(ii) two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with non-Federal records,
(B) but does not include--
(i) matches performed to produce aggregate statistical data without any personal identifiers;

(ii) matches performed to support any research or statistical project, the specific data of which may not be used to make decisions concerning the rights, benefits, or privileges of specific individuals;

(iii) matches performed, by an agency (or component thereof) which performs as its principal function any activity pertaining to the enforcement of criminal laws, subsequent to the initiation of a specific criminal or civil law enforcement investigation of a named person or persons for the purpose of gathering evidence against such person or persons;

(iv) matches of tax information (I) pursuant to section 6103(d) of the Internal Revenue Code of 1986, (II) for purposes of tax administration as defined in section 6103(b)(4) of such Code, (III) for the purpose of intercepting a tax refund due an individual under authority granted by section 404(e), 464, or 1137 of the Social Security Act; or (IV) for the purpose of intercepting a tax refund due an individual under any other tax refund intercept program authorized by statute which has been determined by the Director of the Office of Management and Budget to contain verification, notice, and hearing requirements that are substantially similar to the procedures in section 1137 of the Social Security Act;

(v) matches--

(I) using records predominantly relating to Federal personnel, that are performed for routine administrative purposes (subject to guidance provided

by the Director of the Office of Management and Budget pursuant to subsection (v)); or

(II) conducted by an agency using only records from systems of records maintained by that agency;

if the purpose of the match is not to take any adverse financial, personnel, disciplinary, or other adverse action against Federal personnel; or

(vi) matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of Federal personnel or Federal contractor personnel;

(vii) matches performed incident to a levy described in section 6103(k)(8) of the Internal Revenue Code of 1986; or

(viii) matches performed pursuant to section 202(x)(3) or 1611(e)(1) of the Social Security Act (42 U.S.C. § 402(x)(3), § 1382(e)(1);

(9) the term "recipient agency" means any agency, or contractor thereof, receiving records contained in a system of records from a source agency for use in a matching program;

(10) the term "non-Federal agency" means any state or local government, or agency thereof, which receives records contained in a system of records from a source agency for use in a matching program;

(11) the term "source agency" means any agency which discloses records contained in a system of records to be used in a matching program, or any state or local government, or agency thereof, which discloses records to be used in a matching program;

(12) the term "Federal benefit program" means any program administered or funded by the Federal Government, or by any agent or state on behalf of the Federal Government, providing cash or in-kind assistance in the form of payments, grants, loans, or loan guarantees to individuals; and

(13) the term "Federal personnel" means officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the Government of the United States (including survivor benefits).

(b) Conditions of disclosure

No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another

agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be--

(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;

(2) required under section 552 of this title;

(3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;

(4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of Title 13;

(5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;

(6) to the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value;

(7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;

(8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;

(9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;

(10) to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office;

(11) pursuant to the order of a court of competent jurisdiction; or

(12) to a consumer reporting agency in accordance with section 3711(e) of Title 31.

(c) Accounting of Certain Disclosures

Each agency, with respect to each system of records under its control, shall--

(1) except for disclosures made under subsections (b)(1) or (b)(2) of this section, keep an accurate accounting of--

(A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and

(B) the name and address of the person or agency to whom the disclosure is made;

(2) retain the accounting made under paragraph (1) of this subsection for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made;

(3) except for disclosures made under subsection (b)(7) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request; and

(4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.

(d) Access to records

Each agency that maintains a system of records shall--

(1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence;

(2) permit the individual to request amendment of a record pertaining to him and--

(A) not later than 10 days (excluding Saturdays, Sundays, and legal public holidays) after the date of receipt of such request, acknowledge in writing such receipt; and

(B) promptly, either--

(i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or

(ii) inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official;

(3) permit the individual who disagrees with the refusal of the agency to amend his record to request a review of such refusal, and not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requests such review, complete such review and make a final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after his review, the reviewing official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing official's determination under subsection (g)(1)(A) of this section;

(4) in any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and provide copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed; and

(5) nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

(e) Agency requirements

Each agency that maintains a system of records shall--

(1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive order of the President;

(2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs;

(3) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual--

(A) the authority (whether granted by statute, or by Executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;

(B) the principal purpose or purposes for which the information is intended to be used;

(C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and

(D) the effects on him, if any, of not providing all or any part of the requested information;

(4) subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include--

(A) the name and location of the system;

(B) the categories of individuals on whom records are maintained in the system;

(C) the categories of records maintained in the system;

(D) each routine use of the records contained in the system, including the categories of users and the purpose of such use;

(E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;

(F) the title and business address of the agency official who is responsible for the system of records;

(G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;

(H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and

(I) the categories of sources of records in the system;

(5) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;

(6) prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of this section, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes;

(7) maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity;

(8) make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record;

(9) establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance;

(10) establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained;

(11) at least 30 days prior to publication of information under paragraph (4)(D) of this subsection, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency; and

(12) if such agency is a recipient agency or a source agency in a matching program with a non-Federal agency, with respect to any establishment or revision of a matching program, at least 30 days prior to conducting such program, publish in the Federal Register notice of such establishment or revision.

(f) Agency rules

In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, which shall--

(1) establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him;

(2) define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual;

(3) establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him;

(4) establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his rights under this section; and

(5) establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record.

The Office of the Federal Register shall biennially compile and publish the rules promulgated under this subsection and agency notices published under subsection (e)(4) of this section in a form available to the public at low cost.

(g)(1) Civil remedies

Whenever any agency

(A) makes a determination under subsection (d)(3) of this section not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection;

(B) refuses to comply with an individual request under subsection (d)(1) of this section;

(C) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any

determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual; or

(D) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual, the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.

(2)(A) In any suit brought under the provisions of subsection (g)(1)(A) of this section, the court may order the agency to amend the individual's record in accordance with his request or in such other way as the court may direct. In such a case the court shall determine the matter de novo.

(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

(3)(A) In any suit brought under the provisions of subsection (g)(1)(B) of this section, the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him. In such a case the court shall determine the matter de novo, and may examine the contents of any agency records in camera to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in subsection (k) of this section, and the burden is on the agency to sustain its action.

(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

(4) In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of--

(A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000; and

(B) the costs of the action together with reasonable attorney fees as determined by the court.

(5) An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the

District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where an agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under this section, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action by reason of any injury sustained as the result of a disclosure of a record prior to September 27, 1975.

(h) Rights of legal guardians

For the purposes of this section, the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

(i)(1) Criminal penalties

Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000.

(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.

(j) General exemptions

The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i) if the system of records is--

(1) maintained by the Central Intelligence Agency; or

(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce

crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

(k) Specific exemptions

The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f) of this section if the system of records is--

(1) subject to the provisions of section 552(b)(1) of this title;

(2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: Provided, however, That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

(3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of Title 18;

(4) required by statute to be maintained and used solely as statistical records;

(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

(6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process; or

(7) evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

(1) Archival records

(1) Each agency record which is accepted by the Archivist of the United States for storage, processing, and servicing in accordance with section 3103 of Title 44 shall, for the purposes of this section, be considered to be maintained by the agency which deposited the record and shall be subject to the provisions of this section. The Archivist of the United States shall not disclose the record except to the agency which maintains the record, or under rules established by that agency which are not inconsistent with the provisions of this section.

(2) Each agency record pertaining to an identifiable individual which was transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, prior to the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall not be subject to the provisions of this section, except that a statement generally describing such records (modeled after the requirements relating to records subject to subsections (e)(4)(A)

through (G) of this section) shall be published in the Federal Register.

(3) Each agency record pertaining to an identifiable individual which is transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, on or after the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall be exempt from the requirements of this section except subsections (e)(4)(A) through (G) and (e)(9) of this section.

(m) Government contractors

(1) When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i) of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency.

(2) A consumer reporting agency to which a record is disclosed under section 3711(e) of Title 31 shall not be considered a contractor for the purposes of this section.

(n) Mailing lists

An individual's name and address may not be sold or rented by an agency unless such action is specifically authorized by law. This provision shall not be construed to require the withholding of names and addresses otherwise permitted to be made public.

(o) Matching agreements -- (1) No record which is contained in a system of records may be disclosed to a recipient agency or non-Federal agency for use in a computer matching program except pursuant to a written agreement between the source agency and the recipient agency or non-Federal agency specifying--

(A) the purpose and legal authority for conducting the program;

(B) the justification for the program and the anticipated results, including a specific estimate of any savings;

(C) a description of the records that will be matched, including each data element that will be used, the approximate number of records that will be matched, and the projected starting and completion dates of the matching program;

(D) procedures for providing individualized notice at the time of application, and notice periodically thereafter as directed by the Data Integrity Board of such agency (subject to guidance provided by the Director of the Office of Management and Budget pursuant to subsection (v)), to--

(i) applicants for and recipients of financial assistance or payments under Federal benefit programs, and

(ii) applicants for and holders of positions as Federal personnel, that any information provided by such applicants, recipients, holders, and individuals may be subject to verification through matching programs;

(E) procedures for verifying information produced in such matching program as required by subsection (p);

(F) procedures for the retention and timely destruction of identifiable records created by a recipient agency or non-Federal agency in such matching program;

(G) procedures for ensuring the administrative, technical, and physical security of the records matched and the results of such programs;

(H) prohibitions on duplication and redisclosure of records provided by the source agency within or outside the recipient agency or the non-Federal agency, except where required by law or essential to the conduct of the matching program;

(I) procedures governing the use by a recipient agency or non-Federal agency of records provided in a matching program by a source agency, including procedures governing return of the records to the source agency or destruction of records used in such program;

(J) information on assessments that have been made on the accuracy of the records that will be used in such matching program; and

(K) that the Comptroller General may have access to all records of a recipient agency or a non-Federal agency that the Comptroller General deems necessary in order to monitor or verify compliance with the agreement.

(2)(A) A copy of each agreement entered into pursuant to paragraph (1) shall--

(i) be transmitted to the Committee on Governmental Affairs of the Senate and the Committee on Government Operations of the House of Representatives; and

(ii) be available upon request to the public.

(B) No such agreement shall be effective until 30 days after the date on which such a copy is transmitted pursuant to subparagraph (A)(i).

(C) Such an agreement shall remain in effect only for such period, not to exceed 18 months, as the Data Integrity Board of the agency determines is appropriate in light of the purposes, and length of time necessary for the conduct, of the matching program.

(D) Within 3 months prior to the expiration of such an agreement pursuant to subparagraph (C), the Data Integrity Board of the agency may, without additional review, renew the matching agreement for a current, ongoing matching program for not more than one additional year if--

(i) such program will be conducted without any change; and

(ii) each party to the agreement certifies to the Board in writing that the program has been conducted in compliance with the agreement.

(p) Verification and Opportunity to Contest Findings

(1) In order to protect any individual whose records are used in a matching program, no recipient agency, non-Federal agency, or source agency may suspend, terminate, reduce, or make a final denial of any financial assistance or payment under a Federal benefit program to such individual, or take other adverse action against such individual, as a result of information produced by such matching program, until--

(A)(i) the agency has independently verified the information; or

(ii) the Data Integrity Board of the agency, or in the case of a non-Federal agency the Data Integrity Board of the source agency, determines in accordance with guidance issued by the Director of the Office of Management and Budget that--

(I) the information is limited to identification and amount of benefits paid by the source agency under a Federal benefit program; and

(II) there is a high degree of confidence that the information provided to the recipient agency is accurate;

(B) the individual receives a notice from the agency containing a statement of its findings and informing the individual of the opportunity to contest such findings; and

(C)(i) the expiration of any time period established for the program by statute or regulation for the individual to respond to that notice; or

(ii) in the case of a program for which no such period is established, the end of the 30-day period beginning on the date on which notice under subparagraph (B) is mailed or otherwise provided to the individual.

(2) Independent verification referred to in paragraph (1) requires investigation and confirmation of specific information relating to an individual that is used as a basis for an adverse action against the individual, including where applicable investigation and confirmation of--

(A) the amount of any asset or income involved;

(B) whether such individual actually has or had access to such asset or income for such individual's own use; and

(C) the period or periods when the individual actually had such asset or income.

(3) Notwithstanding paragraph (1), an agency may take any appropriate action otherwise prohibited by such paragraph if the agency determines that the public health or public safety may be adversely affected or significantly threatened during any notice period required by such paragraph.

(q) Sanctions

(1) Notwithstanding any other provision of law, no source agency may disclose any record which is contained in a system of records to a recipient agency or non-Federal agency for a matching program if such source agency has reason to believe that the requirements of subsection (p), or any matching agreement entered into pursuant to subsection (o), or both, are not being met by such recipient agency.

(2) No source agency may renew a matching agreement unless--

(A) the recipient agency or non-Federal agency has certified that it has complied with the provisions of that agreement; and

(B) the source agency has no reason to believe that the certification is inaccurate.

(r) Report on new systems and matching programs

Each agency that proposes to establish or make a significant change in a system of records or a matching program shall provide adequate advance notice of any such proposal (in duplicate) to the Committee on Government Operations of the House of Representatives, the Committee on Governmental Affairs of the Senate, and the Office of Management and

Budget in order to permit an evaluation of the probable or potential effect of such proposal on the privacy or other rights of individuals.

(s) [Biennial report] Repealed by the Federal Reports Elimination and Sunset Act of 1995, Pub. L. No. 104-66, § 3003, 109 Stat. 707, 734-36 (1995), amended by Pub. L. No. 106-113, § 236, 113 Stat. 1501, 1501A-302 (1999) (changing effective date to May 15, 2000).

(t) Effect of other laws

(1) No agency shall rely on any exemption contained in section 552 of this title to withhold from an individual any record which is otherwise accessible to such individual under the provisions of this section.

(2) No agency shall rely on any exemption in this section to withhold from an individual any record which is otherwise accessible to such individual under the provisions of section 552 of this title.

(u) Data Integrity Boards

(1) Every agency conducting or participating in a matching program shall establish a Data Integrity Board to oversee and coordinate among the various components of such agency the agency's implementation of this section.

(2) Each Data Integrity Board shall consist of senior officials designated by the head of the agency, and shall include any senior official designated by the head of the agency as responsible for implementation of this section, and the inspector general of the agency, if any. The inspector general shall not serve as chairman of the Data Integrity Board.

(3) Each Data Integrity Board--

(A) shall review, approve, and maintain all written agreements for receipt or disclosure of agency records for matching programs to ensure compliance with subsection (o), and all relevant statutes, regulations, and guidelines;

(B) shall review all matching programs in which the agency has participated during the year, either as a source agency or recipient agency, determine compliance with applicable laws, regulations, guidelines, and agency agreements, and assess the costs and benefits of such programs;

(C) shall review all recurring matching programs in which the agency has participated during the year, either as a source agency or recipient agency, for continued justification for such disclosures;

(D) shall compile an annual report, which shall be submitted to the head of the agency and the Office of Management and Budget and made available to the public on request, describing the matching activities of the agency, including--

(i) matching programs in which the agency has participated as a source agency or recipient agency;

(ii) matching agreements proposed under subsection (o) that were disapproved by the Board;

(iii) any changes in membership or structure of the Board in the preceding year;

(iv) the reasons for any waiver of the requirement in paragraph (4) of this section for completion and submission of a cost-benefit analysis prior to the approval of a matching program;

(v) any violations of matching agreements that have been alleged or identified and any corrective action taken; and

(vi) any other information required by the Director of the Office of Management and Budget to be included in such report;

(E) shall serve as a clearinghouse for receiving and providing information on the accuracy, completeness, and reliability of records used in matching programs;

(F) shall provide interpretation and guidance to agency components and personnel on the requirements of this section for matching programs;

(G) shall review agency recordkeeping and disposal policies and practices for matching programs to assure compliance with this section; and

(H) may review and report on any agency matching activities that are not matching programs.

(4)(A) Except as provided in subparagraphs (B) and (C), a Data Integrity Board shall not approve any written agreement for a matching program unless the agency has completed and submitted to such Board a cost-benefit analysis of the proposed program and such analysis demonstrates that the program is likely to be cost effective.

(B) The Board may waive the requirements of subparagraph (A) of this paragraph if it determines in writing, in accordance with guidelines prescribed by the Director of the Office of

Management and Budget, that a cost-benefit analysis is not required.

(C) A cost-benefit analysis shall not be required under subparagraph (A) prior to the initial approval of a written agreement for a matching program that is specifically required by statute. Any subsequent written agreement for such a program shall not be approved by the Data Integrity Board unless the agency has submitted a cost-benefit analysis of the program as conducted under the preceding approval of such agreement.

(5)(A) If a matching agreement is disapproved by a Data Integrity Board, any party to such agreement may appeal the disapproval to the Director of the Office of Management and Budget. Timely notice of the filing of such an appeal shall be provided by the Director of the Office of Management and Budget to the Committee on Governmental Affairs of the Senate and the Committee on Government Operations of the House of Representatives.

(B) The Director of the Office of Management and Budget may approve a matching agreement notwithstanding the disapproval of a Data Integrity Board if the Director determines that--

(i) the matching program will be consistent with all applicable legal, regulatory, and policy requirements;

(ii) there is adequate evidence that the matching agreement will be cost- effective; and

(iii) the matching program is in the public interest.

(C) The decision of the Director to approve a matching agreement shall not take effect until 30 days after it is reported to committees described in subparagraph (A).

(D) If the Data Integrity Board and the Director of the Office of Management and Budget disapprove a matching program proposed by the inspector general of an agency, the inspector general may report the disapproval to the head of the agency and to the Congress.

(6) The Director of the Office of Management and Budget shall, annually during the first 3 years after the date of enactment of this subsection and biennially thereafter, consolidate in a report to the Congress the information contained in the reports from the various Data Integrity Boards under paragraph (3)(D). Such report shall include detailed information about costs and benefits of matching programs that are conducted during the period covered by such consolidated report, and shall identify each waiver granted by a Data Integrity Board of the requirement for completion and

submission of a cost-benefit analysis and the reasons for granting the waiver.

(7) In the reports required by paragraphs (3)(D) and (6), agency matching activities that are not matching programs may be reported on an aggregate basis, if and to the extent necessary to protect ongoing law enforcement or counterintelligence investigations.

(v) Office of Management and Budget Responsibilities

The Director of the Office of Management and Budget shall--

(1) develop and, after notice and opportunity for public comment, prescribe guidelines and regulations for the use of agencies in implementing the provisions of this section; and

(2) provide continuing assistance to and oversight of the implementation of this section by agencies.

The following section originally was part of the Privacy Act but was not codified; it may be found at § 552a (note).

Sec. 7(a) (1) It shall be unlawful for any Federal, state or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number.

(2) the provisions of paragraph (1) of this subsection shall not apply with respect to--

(A) any disclosure which is required by Federal statute, or

(B) any disclosure of a social security number to any Federal, state, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.

(b) Any Federal, state or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

The following sections originally were part of P.L. 100-503, the Computer Matching and Privacy Protection Act of 1988; they may be found at § 552a (note).

Sec. 6 Functions of the Director of the Office of Management and Budget.

(b) Implementation Guidance for Amendments -- The Director shall, pursuant to section 552a(v) of Title 5, United States Code, develop guidelines and regulations for the use of agencies in implementing the amendments made by this

Act not later than 8 months after the date of enactment of this Act.

Sec. 9 Rules of Construction.

Nothing in the amendments made by this Act shall be construed to authorize--

(1) the establishment or maintenance by any agency of a national data bank that combines, merges, or links information on individuals maintained in systems of records by other Federal agencies;

(2) the direct linking of computerized systems of records maintained by Federal agencies;

(3) the computer matching of records not otherwise authorized by law; or

(4) the disclosure of records for computer matching except to a Federal, state, or local agency.

Sec. 10 Effective Dates.

(a) In Genera l -- Except as provided in subsection (b), the amendments made by this Act shall take effect 9 months after the date of enactment of this Act.

(b) Exceptions -- The amendment made by sections 3(b) [Notice of Matching Programs -- Report to Congress and the Office of Management and Budget], 6 [Functions of the Director of the Office of Management and Budget], 7 [Compilation of Rules and Notices], and 8 [Annual Report] of this Act shall take effect upon enactment.

APPENDIX F

Georgia Open Records Act[2]

Article 4

Inspection of Public Records

50-18-70. Inspection of public records; printing of computerized indexes of county real estate deed records; time for determination of whether requested records are subject to access.

50-18-71. Right of access to make photographs or reproductions.

50-18-71.1. Approval of judge required for inspection of trial exhibits; reproduction of exhibits.

50-18-71.2 Estimated cost of the copying, search, retrieval, and other administrative fees.

50-18-72. When Public disclosure is not required.

50-18-73. Jurisdiction to enforce article; attorney's fees and litigation expenses; good faith reliance as defense to action.

50-18-74. Unlawful refusal to provide access to public records or to allow copying of such records [repealed].

50-18-75. Confidentiality of communications between Office of Legislative Counsel and certain persons.

50-18-76. Written matter exempt from disclosure under Code Section 31-10-25.

50-18-77. Fee Exemptions

50-18-70.

(a) As used in this article, the term "public records" shall mean all documents, papers, letters, maps, books, tapes, photographs, computer based or generated information, or similar material prepared and maintained or received in the course of the operation of a public office or agency. "Public records" shall also mean such items received or maintained by a private person or entity on behalf of a public office or agency which are not otherwise subject to protection from disclosure. Provided, further, this Code section shall be construed to disallow an agency's placing or causing such items to be placed in the hands of a private

[2] From http://www.sos.state.ga.us/Archives/rms/ora.htm

person or entity for the purpose of avoiding disclosure. Records received or maintained by a private person, firm, corporation, or other private entity in the performance of a service or function for or on behalf of an agency, a public agency, or a public office shall be subject to disclosure to the same extent that such records would be subject to disclosure if received or maintained by such agency, public agency, or public office. As used in this article, the term "agency" or "public agency" shall have the same meaning and application as provided for in the definition of the term "agency" in paragraph (1) of subsection (a) of Code Section 50-14-1 and shall additionally include any association, corporation, or other similar organization which:

(1) has a membership or ownership body composed primarily of counties, municipal corporations, or school districts of this state or their officers or any combination thereof: and

(2) derives a substantial portion of its general operating budget from payments from such political subdivisions.

(b) All public records of an agency as defined in subsection (a), except those which by order of a court of this state or by law are prohibited or specifically exempted from being open to inspection by the general public, shall be open for a personal inspection by any citizen of this state at a reasonable time and place; and those in charge of such records shall not refuse this privilege to any citizen.

(c) Any computerized index of a county real estate deed records shall be printed for purposes of public inspection no less than every 30 days and any correction made on such index shall be made a part of the printout and shall reflect the time and date that said index was corrected.

(d) No public officer or agency shall be required to prepare reports , summaries, or compilations not in existence at the time of the request.

(e) In a pending proceeding under Chapter 13 of this title, the "Georgia Administrative Procedures Act," or under any other administrative proceeding authorized under Georgia law, a party may not access public records pertaining to the subject of the proceeding pursuant to this article without the prior approval of the presiding administrative law judge, who shall consider such open record request in the same manner as any other request for information put forth by a party in such a proceeding. This subsection shall not apply to any proceeding under Chapter 13 of this title, relating to the revocation, suspension, annulment, withdrawal, or denial of a professional education certificate, as defined in Code Section 20-2-200, or any personnel proceeding authorization under Part 7 and Part 11 of Article 17 and Article 25 of Chapter 2 of Title 20.

(f) The individual in control of such public record or records shall have a reasonable amount of time to determine whether or not the record or records requested are subject to access under this article and to permit inspection and copying. In no event shall this time exceed three business days. Where responsive records exist but are not available within three business days of the request, a

written description of such records, together with a timetable for their inspection and copying, shall be provided within that period; provided, however, that records not subject to inspection under this article need not be made available for inspection and copying or described other than as required by subsection (h) of Code Section 50-18-72, and no records need be made available for inspection or copying if the public officer or agency in control of such records shall have obtained, within that period of three business days, an order based on an exception in this article of a superior court of this state staying or refusing the requested access to such records.

(g) At the request of the person, firm, corporation, or other entity requesting such records, records maintained by computer shall be made available where practicable by electronic means, including Internet access, subject to reasonable security restrictions preventing access to non-requested or non-available records.

50-18-71.

(a) In all cases where an interested member of the public has a right to inspect or take extracts or make copies from any public records, instruments, or documents, any such person shall have the right of access to the records, documents, or instruments for the purpose of making photographs or reproductions of the same while in the possession, custody, and control of the lawful custodian thereof, or his authorized deputy. Such work shall be done under the supervision of the lawful custodian of the records, who shall have the right to adopt and enforce reasonable rules governing the work. The work shall be done in the room where the records, documents, or instruments are kept by law. While the work is in progress, the custodian may charge the person making the photographs or reproductions of the records, documents, or instruments at a rate of compensation to be agreed upon by the person making the photographs and the custodian for his services of the services of a deputy in supervising the work.

(b) Where fees for certified copies or other copies or records are specifically authorized or otherwise prescribed by law, such specific fee shall apply.

(c) Where no fee is otherwise provided by law, the agency may charge and collect a uniform copying fee not to exceed 25 [cents] per page.

(d) In addition, a reasonable charge may be collected for search, retrieval, and other direct administrative costs for complying with a request under this Code section. The hourly charge shall not exceed the salary of the lowest paid full-time employee who, in the discretion of the custodian of the records, has the necessary skill and training to perform the request; provided, however, that no charge shall be made for the first quarter hour.

(e) An agency shall utilize the most economical means available for providing copies of public records.

(f) Where information requested is maintained by computer, an agency may charge the public its actual cost of a computer disk or tape onto which the

information is transferred and may charge for the administrative time involved as set forth in subsection (d) of this Code section.

50-18-71.1

(a) Notwithstanding any other provision of this article, an exhibit tendered to the court as evidence in a criminal or civil trial shall not be open to public inspection without approval of the judge assigned to the case or, if no judge has been assigned, approval of the chief judge, or if nor judge has been designated chief judge, approval of the judge most senior in length of service on the court.

(b) In the event inspection is not approved by the court, in lieu of inspection of such exhibit, the custodian of such an exhibit shall, upon request, provide one or more of the following representations of the exhibit:

(1) A photograph;

(2) A photocopy;

(3) A facsimile; or

(4) Another reproduction.

(c) The provision of subsections (b), (c), (d), and (e) of Code Section 50-18-71 shall apply to fees, costs, and charges for providing a photograph, facsimile, or other reproduction of such exhibit shall not exceed the cost of materials or supplies and a reasonable charge for time spent producing the photograph, facsimile, or other reproduction, in accordance with subsection (d) and (e) of Code Section 50-18-71.

50-18-71.2

Any agency receiving a request for public records shall be required to notify the party making the request of the estimated cost of the copying, search, retrieval, and other administrative fees authorized by Code Section 50-18-71 as a condition of compliance with the provisions of this article prior to fulfilling the request as a condition for assessment of any fee; provided, however, that no new fees other than those directly attributable to providing access shall be assessed where records are made available by electronic means.

50-18-72

When public disclosure not required; disclosure of exempting legal authority.

(a) Public disclosure shall not be required for records that are:

(1) Specifically required by the federal government to be kept confidential;

(2) Medical or veterinary records and similar files, the disclosure of which would be an invasion of personal privacy;

(3) Except as otherwise provided by law, records compiled for law enforcement or prosecution purposes to the extent that production of such records would disclose the identity of a confidential source, disclose confidential investigative or prosecution material which would endanger the life or physical safety of any person or persons, or disclose the existence of a confidential surveillance or investigation;

(4) Records of law enforcement, prosecution, or regulatory agencies in any pending investigation or prosecution of criminal or unlawful activity, other than initial police arrest reports, and initial incident reports; provided, however, that an investigation or prosecution shall no longer be deemed to be pending when all direct litigation involving said investigation and prosecution has become final or otherwise terminated;

(4.1) Individual Georgia Uniform Motor Vehicle Accident Reports, except upon the submission of a written statement of need by the requesting party, such statement to be provided to the custodian of records and to set forth the need for the report pursuant to this Code section; provided, however, that any person or entity whose name or identifying information is contained in a Georgia Uniform Motor Vehicle Accident report shall be entitled, either personally or through a lawyer or other representative, to receive a copy of such report; and provided further that Georgia Uniform Motor Vehicle Accident reports shall not be available in bulk for inspection or copying by any person absent a written statement showing the need for each such report pursuant to the requirements of this Code section. For the purposes of this subsection, the term 'need' means that the natural person or legal entity who is representing in person or by representative to inspect or copy the Georgia Uniform Motor Vehicle Accident Report:

(A) Has a personnel, professional, or business connection with a party to the accident;

(B) Owns or leases an interest in property allegedly or actually damaged in the accident;

(C) Was allegedly or actually injured by the accident;

(D) Was a witness to the accident;

(E) Is the actual or alleged insurer of a party to the accident or of property actually or allegedly damaged by the accident;

(F) Is a prosecutor or publicly employed law enforcement officer;

(G) Is alleged to be liable to another party as a result of the accident;

(H) Is an attorney stating that he or she needs the requested reports as part of a criminal case, or an investigation of a potential claim involving contentions that a roadway, railroad crossing, or intersection is unsafe;

(I) Is gathering information as a representative of a news media organization; or

(J) Is conducting research in the public interest for such purposes as accident prevention, prevention of injuries or damages in accidents, determination of fault in an accident or accidents, or other similar purposes; provided, however, this subparagraph will apply only to accident reports on accidents that occurred more than 30 days prior to the request and which shall have the name, street address,telephone number and driver's license number redacted.

(5) Records that consist of confidential evaluations submitted to, or examinations prepared by, a governmental agency and prepared in connection with the appointment or hiring of a public officer or employee; and records consisting of material obtained in investigations related to the suspension, firing, or investigation of complaints against public officers or employees until ten days after the same has been presented to the agency or an officer for action or the investigation is otherwise concluded or terminated, provided that this paragraph shall not be interpreted to make such investigatory records privileged.

(6) (A) Real estate appraisals, engineering or feasibility estimates, or other records made for or by the state or a local agency relative to the acquisition of real property until such time as the property has been acquired or the proposed transaction has been terminated or abandoned;

(B) and engineers cost estimates and rejected or deferred bid proposals until such time as the final award is made, either received or prepared by the Department of Transportation pursuant to Article 4 of Chapter 2 of Title 32, by a county pursuant to Article 3 of Chapter 4 of Title 32, or by a municipality pursuant to Article 4 of Chapter 4 of Title 32:

(7) Notwithstanding any other provision of this article, an agency shall not be required to release those portions of records which would identify persons applying for or under consideration for employment or appointment as executive head of an agency as that term is defined in paragraph (1) of subsection (a) of Code Section 50-14-1, or of a unit of the University System of Georgia; provided, however, that at least 14 calendar days prior to the meeting at which final action or vote is to be taken on the position, the agency shall release all documents which came into its possession with respect to as many as three persons under consideration whom the agency has determined to be the best qualified for the position and from among whom the agency intends to fill the position. Prior to the release of these documents, an agency may allow such a person to decline being considered further for the position rather than have documents pertaining to the person released. In that event, the agency shall release the documents of the next most qualified person under consideration who does not decline the position. If an agency has conducted its hiring or appointment process open to the public, it shall not be required to delay 14 days to take final action on the

position. The agency shall not be required to release such records with respect to other applicants or persons under consideration, except at the request of any such person. Upon request, the hiring agency shall furnish the number of applicants and the composition of the list by such factors as race and sex. Provided, further, the agency shall not be allowed to avoid the provisions of this paragraph by the employment of a private person or agency to assist with the search or application process;

(8) Related to the provision of staff services to individual members of the General Assembly by the Legislative and Congressional Reapportionment Office, the Senate Research Office, or the House Research Office, provided that this exception shall not have any application with respect to records related to the provision of staff services to any committee or subcommittee or to any records which are or have been previously publicly disclosed by or pursuant to the direction of an individual member of the General Assembly; or

(9) Records that are of historical research value which are given or sold to public archival institutions, public libraries, or libraries of a unit of the Board of Regents of the University System of Georgia when the owner or donor of such records wishes to place restrictions on access to the records. No restriction on access, however, may extend more than 75 years from the date of donation or sale. This exemption shall not apply to any records prepared in the course of the operation of state or local governments of the State of Georgia.

(10) Records that contain information from the Department of Natural Resources inventory and register relating to the location and character of a historic property of historic properties as those terms are defined in Code Sections 12-3-50.1 and 12-3-50.2 if the Department of Natural resources through its Division of Historic Preservation determines that disclosure will create a substantial risk of harm, theft, or destruction to the property or properties or the area or place where the property or properties are located; or

(11) Records that contain site specific information regarding the occurrence of rare species of plants or animals or the location of sensitive natural habitats on public or private property if the Department of Natural Resources determines that disclosure will create a substantial risk of harm, theft, or destruction to the species or habitats or the area or place where the species or habitats are located; provided, however, that the owner or owners of private property upon which rare species of plants or animals are located shall be entitled to such information pursuant to this article.

(11.1) An individual's social security number and insurance or medical information in personnel records, which my be redacted from such records;

(11.2) Records that would reveal the names, home addresses, telephone numbers, security codes, or any other data or information developed, collected, or received by counties or municipalities in connection with the installation, servicing, maintaining, operating, selling, or leasing of burglar alarm systems, fire alarm systems, or other electronic security systems; provided, however, that initial

police reports and initial incident reports shall remain subject to disclosure pursuant to paragraph (4) of this subsection;

(11.3)

A. An individual's social security number, mother's birth name, credit card information, debit card information, bank account information, financial data or information, and insurance or medical information in all records, and if technically feasible at reasonable cost, day and month of birth, which shall be redacted prior to disclosure of any record requested pursuant to this article; provided, however, that such information shall not be redacted from such records if the person or entity requesting such records requests such information in a writing signed under oath by such person or a person legally authorized to represent such entity which states that such person or entity is gathering information as a representative of a news media organization for use in connection with news gathering and reporting; and provided, further, that such access shall be limited to social security numbers and day and month of birth; and provided, further, that this news media organization exception for access to social security numbers and day and month of birth and the other protected information set forth in this subparagraph shall not apply to teachers and employees of a public school.

Formatted: Bullets and Numbering

B. This paragraph shall have no application to:

i. The disclosure of information contained in the records or papers of any court or derived therefrom including without limitation records maintained pursuant to Article 9 of Title 11;

ii. The disclosure of information to a court, prosecutor, or publicly employed law enforcement officer, or authorized agent thereof, seeking records in an official capacity;

iii. The disclosure of information to a public employee of this state, its political subdivisions, or the United States who is obtaining such information for administrative purposes, in which case, subject to applicable laws of the United States, further access to such information shall continue to be subject to the provisions of this paragraph;

iv. The disclosure of information as authorized by the order of a court of competent jurisdiction upon good cause shown to have access to any or all of such information upon such conditions as may be set forth in such order;

v. The disclosure of information to the individual in respect of whom such information is maintained, with the authorization thereof, or to an authorized agent thereof; provided, however, that the agency maintaining such information shall require proper identification of such individual or such individual's agent, or proof of authorization, as determined by such agency;

vi. The disclosure of the day and month of birth and mother's birth name of a deceased individual;

vii. The disclosure by an agency of credit or payment information in connection with a request by a consumer reporting agency as that term is defined under the federal Fair Credit Reporting Act (15 U.S.C. Section 1681, et seq.);

viii. The disclosure by an agency of information in its records in connection with the agency's discharging or fulfilling of its duties and responsibilities, including, but not limited to, the collection of debts owed to the agency or individuals or entities whom the agency assists in the collection of debts owed to the individual or entity; or

ix. The disclosure of information necessary to comply with legal or regulatory requirements or for legitimate law enforcement purposes.

C. Records and information disseminated pursuant to this paragraph may be used only by the authorized recipient and only for the authorized purpose. Any person who obtains records or information pursuant to the provisions of this paragraph and knowingly and willfully discloses, distributes, or sells such records or information to an unauthorized recipient or for an unauthorized purpose shall be guilty of a misdemeanor of a high and aggravated nature and upon conviction thereof shall be punished as provided in Code Section 17-10-4. Any person injured thereby shall have a cause of action for invasion of privacy. Any prosecution pursuant to this paragraph shall be in accordance with the procedure in subsection (b) of Code Section 50-18-74.

D. In the event that the custodian of public records protected by this paragraph has good faith reason to believe that a pending request for such records has been made fraudulently, under false pretenses, or by means of false swearing, such custodian shall apply to the superior court of the county in which such records are maintained for a protective order limiting or prohibiting access to such records.

E. This paragraph shall supplement and shall not supplant, overrule, replace, or otherwise modify or supersede any provision of statute, regulation, or law of the federal government or of this state as now or hereafter amended or enacted requiring, restricting, or prohibiting access to the information identified in subparagraph (A) of this paragraph and shall constitute only a regulation of the methods of such access where not otherwise provided for, restricted, or prohibited;

(12) Public records containing information that would disclose or might lead to the disclosure of any component in the process used to execute or adopt an electronic signature, if such disclosure would or might cause the electronic signature to cease being under the sole control of the person using it. For purposes of this paragraph, the term "electronic signature" has the same meaning as that term is defined in Code Section 10-12-3; or

(13) Records that would reveal the home address or telephone number, social security number, or insurance or medical information of law enforcement officers, judges, scientists employed by the Division of Forensic Sciences of the Georgia Bureau of Investigation, correctional employees, and prosecutors or identification of immediate family members or dependents thereof.

(13.1) Records that reveal the home address, the home telephone number, or the social security number of or insurance or medical information about teachers and employees of a public school. For the purposes of this paragraph, the term "public school" means any school which is conducted within this state and which is under the authority and supervision of a duly elected county or independent board of education;

(14) Acquired by an agency for the purpose of establishing or implementing, or assisting in the establishment or implementation of, a carpooling or ridesharing program, to the extent such records would reveal the name, home address, employment address, home telephone number, employment telephone number, or hours of employment of any individual or would otherwise identify any individual who is participating in, or who has expressed an interest in participating in, any such program. As used in this paragraph, the term "carpooling or ridesharing program" means and includes, but is not limited to, the formation of carpools, vanpools, or buspools, the provision of transit routes, rideshare research, and the development of other demand management strategies such as variable working hours and telecommuting;

(15)

A. Records, the disclosure of which would compromise security against sabotage or criminal or terrorist acts and the nondisclosure of which is necessary for the protection of life, safety, or public property, which shall be limited to the following:

Formatted: Bullets and Numbering

i. Security plans and vulnerability assessments for any public utility, technology infrastructure, building, facility, function, or activity in effect at the time of the request for disclosure or pertaining to a plan or assessment in effect at such time;

ii. Any plan for protection against terrorist or other attacks, which plan depends for its effectiveness in whole or in part upon a lack of general public knowledge of its details;

iii. Any document relating to the existence, nature, location, or function of security devices designed to protect against terrorist or other attacks, which devices depend for their effectiveness in whole or in part upon a lack of general public knowledge; and

iv. Any plan, blueprint, or other material which if made public could compromise security against sabotage, criminal, or terroristic acts.

B. In the event of litigation challenging nondisclosure pursuant to this paragraph by an agency of a document covered by this paragraph, the court may review the documents in question in camera and may condition, in writing, any disclosure upon such measures as the court may find to be necessary to protect against endangerment of life, safety, or public property.

C. As used in divisions (i) and (iv) of subparagraph (A) of this paragraph, the term "activity" means deployment or surveillance strategies, actions mandated by changes in the federal threat level, motorcades, contingency plans, proposed or alternative motorcade routes, executive and dignitary protection, planned responses to criminal or terrorist actions, after-action reports still in use, proposed or actual plans and responses to bioterrorism, and proposed or actual plans and responses to requesting and receiving the National Pharmacy Stockpile; or

(16) Unless the request is made by the accused in a criminal case or by his or her attorney, public records of an emergency "911" system, as defined in paragraph (3) of Code Section 46-5-122, containing information which would reveal the name, address, or telephone number of a person placing a call to a public safety answering point, which information may be redacted from such records if necessary to prevent the disclosure of the identity of a confidential source, to prevent disclosure of material which would endanger the life or physical safety of any person or persons, or to prevent the disclosure of the existence of a confidential surveillance or investigation.

(b) This article shall not be applicable to:

(1) Any trade secrets obtained from a person or business entity which are of a privileged or confidential nature and required by law to be submitted to a government agency or to data, records, or information of a proprietary nature, produced or collected by or for faculty or staff of state institutions of higher learning, or other governmental agencies, in the conduct of or as a result of, study or research on commercial, scientific, technical, or scholarly issues, whether sponsored by the institution alone or in conjunction with a governmental body or private concern, where such data, records, or information has not been publicly released, published, copyrighted, or patented; or

(2) Any data, records, or information developed, collected, or received by or on behalf of faculty, staff, employees, or students of an institution of higher education or any public or private entity supporting or participating in the

activities of an institution of higher education in the conduct of, or as a result of, study or research on medical, scientific, technical, scholarly, or artistic issues, whether sponsored by the institution alone or in conjunction with a governmental body or private entity until such information is published, patented, otherwise publicly disseminated, or released to an agency whereupon the request must be made to the agency. This subsection applies to, but is not limited to, information provided by participants in research, research notes and data, discoveries, research projects, methodologies, protocols, and creative works; or

(3) Unless otherwise provided by law, contract, bid, or proposal, records consisting of questions, scoring keys, and other materials, constituting a test that derives value from being unknown to the test taker prior to administration, which is to be administered by the State Board of Education, the Office of Education Accountability, or a local school system, if reasonable measures are taken by the owner of the test to protect security and confidentiality; provided, however, that the State Board of Education may establish procedures whereby a person may view, but not copy, such records if viewing will not, in the judgment of the board, affect the result of administration of such test. These limitations shall not be interpreted by any court of law to include or otherwise exempt from inspection the records of any athletic association or other nonprofit entity promoting intercollegiate athletics.

(c) (1) All public records of hospital authorities shall be subject to this article except f or those otherwise excepted by this article or any other provision of law.

(2) All state officers and employees shall have a privilege to refuse to disclose the identity or personally identifiable information of any person participating in research on commercial, scientific, technical, medical, scholarly, or artistic issues conducted by the Department of Human Resources or state institution of higher education whether sponsored by the institution alone or in conjunction with a governmental body or private entity. Personally identifiable information shall mean any information which if disclosed might reasonably reveal the identity of such person including but not limited to the person's name, address, and social security number. The identity of such information shall not be admissible in evidence in any court of the state unless the court finds that the identity of the informant already has been disclosed otherwise.

(d) This article shall not be applicable to any application submitted to or any permanent records maintained by a judge of the probate court pursuant to Code Section 16-11-129, relating to licenses to carry pistols or revolvers, or pursuant to any other requirement for maintaining records relative to the possession of firearms. This subsection shall not preclude law enforcement agencies from obtaining records relating to licensing and possession of firearms as provided by law.

(e) This article shall not be construed to repeal:

(1) The attorney-client privilege recognized by state law to the extent that a record pertains to the requesting or giving of legal advice or the disclosure of facts concerning or pertaining to pending or potential litigation, settlement, claims, administrative proceedings, or other judicial actions brought or to be brought by or against the agency or any officer or employee; provided, however, attorney-client information may be obtained in a proceeding under Code Section 50-18-73 to prove justification or lack thereof in refusing disclosure of documents under this Code section provided the judge of the court in which said proceeding is pending shall first determine by an in camera examination that such disclosure would be relevant on that issue;

(2) The confidentiality of attorney work product; or

(3) State laws making certain tax matters confidential.

(f) (1) As used in this article, the term;

(A) Computer program" means a set of instructions, statements, or related data that, in actual or modified form, is capable of causing a computer or computer system to perform specified functions.

(b) Computer software" means one or more computer programs, existing in any form, or any associated operational procedures, manuals, or other documentation.

(2) This article shall not be applicable to any computer program or computer software used or maintained in the course of operation of a public office or agency.

(g) This Code section shall be interpreted narrowly so as to exclude from disclosure only that portion of a public record to which an exclusion is directly applicable. It shall be the duty of the agency having custody of a record to provide all other portions of a record for public inspection or copying.

(h) Within the three business days applicable to response to a request for access under this article, the public officer or agency having control of such record or records, if access to such record or records is denied in whole or in part, shall specify in writing the specific legal authority exempting such record or records from disclosure, by Code section, subsection, and paragraph. No addition to or amendment of such designation shall be permitted thereafter or in any proceeding to enforce the terms of this article; provided, however, that such designation may be amended or supplemented one time within five days of discovery of an error in such designation or within five days of the institution of an action to enforce this chapter, whichever is sooner; provided, further that the right to amend or supplement based upon discovery of an error may be exercised on only one occasion. In the event that such designation includes provisions not relevant to the subject matter of the request, costs, and reasonable attorney's fees may be awarded pursuant to Code Section 50-18-73.

50-18-73.

(a) The superior courts of this state shall have jurisdiction in law and in equity to entertain actions against persons or agencies having custody of records open to the public under this article to enforce compliance with the provisions of this article. Such actions may be brought by any person, firm, corporation, or other entity.

(b) In any action brought to enforce the provisions of this chapter in which the court determines that either party acted without substantial justification either in not complying with this chapter or in instituting the litigation, the court shall, unless it finds that special circumstances exist, assess in favor of the complaining party reasonable attorney's fees and other litigation costs reasonably incurred. Whether the position of the complaining party was substantially justified shall be determined on the basis of the record as a whole which is made in the proceeding for which fees and other expenses are sought.

(c) Any agency or person who provides access to information in good faith reliance on the requirements of this chapter shall not be liable in any action on account of having provided access to such information.

50-18-74.

(a) Any person knowingly and willfully violating the provisions of this article by failing or refusing to provide access to records not subject to exemption from this article or by failing or refusing to provide access to records within the time limits set forth in this article shall be guilty of a misdemeanor and upon conviction shall be punished by a fine not to exceed $100.00.

(b) A prosecution under this Code section may only be commenced by issuance of a citation in the same manner as an arrest warrant for a peace officer pursuant to Code Section 17-4-40, which citation shall be personally served upon the accused. The defendant shall not be arrested prior to the time of trial, except that a defendant who fails to appear for arraignment or trial may thereafter be arrested pursuant to a bench warrant and required to post a bond for his or her future appearance.

50-18-75.

Communications between the Office of Legislative Counsel and the following persons shall be privileged and confidential: members of the General Assembly, the Lieutenant Governor, and persons acting on behalf of such public officers; and such communications, and records and work product relating to such communications, shall not be subject to inspection or disclosure under this article or any other law or under judicial process; provided, however, that this privilege shall not apply where it is waived by the affected public officer or officers. The privilege established under this Code section is in addition to any other constitutional, statutory, or common law privilege.

50-18-76.

No form, document, or other written matter which is required by law or rule or regulation to be filed as a vital record under the provisions of Chapter 10 of Title 31, which contains information which is exempt from disclosure under Code Section 31-10-25, and which is temporarily kept of maintained in any file or with any other documents in the office of the judge or clerk of any court prior to filing with the Department of Human Resources shall be open to inspection by the general public, even though the other papers or documents in such file may be open to inspection.

50-18-77.

The procedures and fees provided for in this article shall not apply to public records, including records that are exempt from disclosure pursuant to Code Section 50-18-72, which are requested in writing by a state or federal grand jury, taxing authority, law enforcement agency, or prosecuting attorney in conjunction with an ongoing administrative criminal, or tax investigation. The lawful custodian shall provide copies of such records to the requesting agency unless such records are privileged or disclosure to such agencies is specifically restricted by law.

APPENDIX G

How to Remain Open in a Closed Standards World

I. What are Open Standards?

The perception of what constitutes an open standard has changed dramatically as the players and focus of the industry have changed over time. In the 1980's to say that a system adhered to open standards meant that is was an IBM-compatible and ran a version of DOS. This was in contrast to the Macintosh which was a closed system or proprietary system where a single vendor provided both the operating system and the hardware. The IBM-compatible systems emulated the functions of the orginal IBM PC and ran an operating system that was provided by IBM, Microsoft or Dr. DOS. Because they all adhered to certain technical specifications or standards, systems from different vendors were capable of running the same software. However it is important to note that there was never an "official" standard defining the characteristics of an IBM-compatible instead it was a de-facto standard created when IBM chose to use off the shelf components to create its PC and did not challenge competitors when they reversed engineered the sole proprietary component of the PC, the BIOS.

Since the 1980's, the focus of the computer industry has shifted from hardware to software. Likewise so has the perception of what comprises an open standard. Two parallel trends occurred during the early 1990's. The first was the dominance of the Microsoft Windows Operating System and the second was the rise of standards bodies that focused primarily on application level protocols such as W3C, OASIS and WS-I. Windows provided a common environment for building applications and in doing so spawned a multi-billion dollar software industry. Windows was also a closed system strictly controlled by the vendor. One of the business strategies for Microsoft was to ensure that the applications it built worked only on its operating system. In addition Microsoft developed its own application level protocols that were not supported by other vendors and in some cases, re-invented the wheel. These actions by Microsoft fostered the idea that the Windows environment was a completely closed system.

Like Microsoft there were a number of vendors with their own operating system, but they were based on UNIX and POSIX, technologies originally developed by AT&T Bell Labs and later standardized through a standards body. The intention of these standards was to ensure that vendors of different UNIX implementations would be compatible (i.e. able to run the same software). However, each UNIX vendor added additional features that were unique to their version of UNIX making the promise of instant code portability more theory than practice. But because these UNIX

implementations supposedly adhered to standards they were deemed to be more open than closed operating systems such as Microsoft Windows.

The story of JAVA-based application servers is essentially the same story as UNIX. Each vendor adds their own "value-added" features that make portability between different servers fairly difficult, but doable. Allowing each to claim adherence to a relatively open standard (JAVA is controlled by SUN through the JAVA Community Process (JCP)), each vendor ensures that clients who take advantage of their product specific features are effectively locked-in to that particular vendor's implementation of the JAVA-based application server.

The point of this discussion is to show that standards are very real, but there are de-facto standards based upon the popularity of a product and explicit standards agreed upon by a community of vendors with widely varying implementations that can render the standard ineffective. De-facto standards are simply a fact life and must be considered whenever a technology decision is made. Explicit standards can be effective when the implementation of the standard is controlled either at design-time or at deployment-time.

II. Data Categorization and Open Standards

In the area of data categorization there are three types of technical standards to consider data security, data definition and data interoperability. Technical data security standards define how the user gains access to the data. This may include network technologies such as VPN and application level security technologies such as SAML (Security Assertion Markup Language). Technical standards regarding data definition allow for the portability of the context and definition of the data between disparate systems. Examples of these standards include CORBA definition objects, ADO Components, JAVA Objects and XML schemas. Lastly, there are technical standards for data interoperability these standards allow for data to pass seamlessly between systems. Examples include Web Services, JAVA RMI, IIOP and COM+.

III. Technologies to Consider

In regards to data the industry has pretty well aligned itself with XML and XML-based technologies such as Web Services to deliver at the application level, data security, data definitions and data interoperability. There are two principle technology platforms designed to implement these technologies they are Microsoft's .NET products and J2EE (JAVA 2 Enterprise Edition) based products. To-date the only commercial products to support .NET are those from Microsoft. By leveraging its extensive existing development community and Windows and Office install base, .NET has become a de-facto standard in the industry. The JAVA sphere is more diverse with players of various sizes with leaders being IBM and BEA. Gartner has projected that by 2006 nearly

50% of all enterprise development will be .NET-based development with a corresponding 50% will be JAVA-based development.

IV. The Open Source Question

The open source community often provides the "purest" implementations of standards simply because of its near religious zealotry for openness. In fact often times an open source technology can become the de-facto standard and be included in commercial products. The Apache Web Server is the best example of this phenomenon, but it is not alone both JBOSS and the ORION application servers have been included in products from WebMethods and Oracle respectively. Open source tools often provide a cost effective way to implement technical standards. These tools are oftentimes several months faster at delivering an implementation of the latest standard.

V. Recommendations

In order to ensure the openness of data between state systems openness in regards to data must be defined. The most immediate definition is that data openness means that data is portable between systems. In order for data to be portable there must be agreed upon standards for data security and data interoperability and common data definitions. Fortunately there are a number of technical standards to define data and ensure interoperability particularly in the areas of XML and Web Services. However, data security with XML and Web Services is still relatively new. Below are several specific recommendations to help address this problem;

1. Employee agreed upon technical standard stacks such as the WS-I Basic Profile. WS-I has defined a group of technical standards for Web Services that all of the major vendors have agreed to implement the same way.
2. Do not employee product specific features that are incompatible with other products. This does not mean avoid all product specific features, but rather to eliminate incompatibilities when attempting to share data by not utilizing features that effect data sharing.
3. Rather then implement a vendor's specific implementation; develop a custom scheme for handling functionality where the technical standard stack is still immature. Make the vendors whose products are involved aware of the work to ensure a planned migration path to the standard when it is available.
4. Limit the deployment of products to a manageable level to allow for the development of internal communities of experts.

These recommendations should assist in the overcoming some of the immediate limitations in the technical standards for Web Services as well as address some of the realities of data openness in a diverse technical environment.

APPENDIX H

Privacy and Access Conference
Agenda

Privacy & Access in Georgia E-Government
Conference Agenda
July 2003

July 16

9:15 – 9:30	Welcome & Overview of Topics and Goals David W. Carmicheal, Georgia Archives
9:30 – 10:45	Ground Rules for Conference Dr. Richard Halstead-Nussloch, SPSU
10:45 – 11:00	Break
11:00 -11:45	Policy Perspectives on Government Use of Citizen Data: Balancing the Need for Privacy Dr. Paul M.A. Baker, Georgia Centers for Advanced Telecommunications Technology Richard Keck, JD, Troutman Sanders Law Firm
11:45 – 1:00	Lunch
1:00 – 2:00	Policy Perspectives on Government Use of Citizen Data: Balancing the Need for Privacy Dr. Paul M.A. Baker, Georgia Centers for Advanced Telecommunications Technology Richard Keck, JD, Troutman Sanders Law Firm
2:00 – 2:15	Break
2:15 – 3:00	Discussion Dr. Richard Halstead-Nussloch, facilitator

July 17

9:00 – 9:15	Welcome and Introduction of Speakers
9:15 – 10:15	Let's Not Reinvent the Wheel: New Jersey as an Example

Odysseus Marcopolus and Paula Arcioni, New Jersey, Office of E-Government Services

10:15 – 10:30	Break
10:30 – 11:15	Let's Not Reinvent the Wheel: New Jersey as an Example Odysseus Marcopolus and Paula Arcioni, New Jersey, Office of E-Government Services
11:15 – 11:45	Discussion Dr. Richard Halstead-Nussloch, facilitator
11:45 – 1:00	Lunch
1:00 – 2:30	Laws, Rules, and Regulations Impacting Georgia E-Government Kathryn Allen, Office of Attorney General
2:30 – 2:45	Break
2:45 – 3:30	Discussion Dr. Richard Halstead-Nussloch, facilitator

July 23

9:00 – 9:15	Welcome and Introduction of Speaker
9:15 - 10:00	Digital Identity: A Discussion Emily Frye, George Mason University
10:00 – 10:15	Break
10:15 – 11:15	Digital Identity: A Discussion Emily Frye, George Mason University
11:15 – 11:45	Discussion Dr. Richard Halstead-Nussloch, facilitator
11:45 – 1:00	Lunch
1:00 – 2:30	Digital Identity: A Discussion Emily Frye, George Mason University
2:30 – 2:45	Break
2:45 – 3:45	Discussion Dr. Richard Halstead-Nussloch, facilitator

July 24

9:00 – 9:15	Welcome and Introduction of Speakers
9:15 – 10:30	Planning for the Long-Term: When Digital Identity and E-Records Must be Maintained Dr. Charles Dollar, Dollar Consulting
10:30 – 10:45	Break
10:45 – 11:45	Discussion Dr. Richard Halstead-Nussloch, facilitator
11:45 – 1:00	Lunch
1:00 – 2:30	Lifecycle Management of Georgia's E-Records Andrew S. Taylor, Georgia Archives
2:30 – 2:45	Break
2:45 – 3:45	Discussion

July 30 and 31

9:15 – 9:30	Conference Wrap-up Amelia Winstead & Dr. Richard Halstead-Nussloch
9:30 – 10:45	Review of Georgia Rules, Elements of Digital Identity, and Lifecycle Management
10:45 – 11:00	Break
11:00 -11:45	Review of Georgia Rules, Elements of Digital Identity, and Lifecycle Management
11:45 – 1:00	Lunch
1:00 – 2:00	Review of Georgia Rules, Elements of Digital Identity, and Lifecycle Management
2:00 – 2:15	Break
2:15 – 3:00	Outline of White Paper