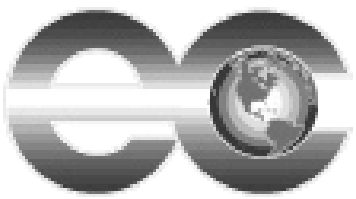
Critical Business Issues
In the
Transformation to Electronic Government

NECCC
December, 2000



NECCC
EXECUTIVE BOARD

Chair
J.D. Williams, ID
NASACT

Vice Chair
Richard B. Thompson, ME
NASPO

Secretary/Treasurer
Carolyn Purcell, TX
NASIRE

NECCC BOARD

NASIRE:
Otto Doll, SD

NASPO:
Dave Ancell, MI
Joyce Murphy, MO

NASS:
Elaine Marshall, NC
Ken Blackwell, OH
Ron Thornburgh, KS

NASACT:
David Heineman, NE
R. Thomas Wagner, DE

NGA:

NASCA:
Pam Aherns, ID

ITAA:
Basil Nikas

NACHA:
Bill Kilmartin

The National Electronic Commerce Coordinating Council (NECCC)

The NECCC is an alliance of national state government associations dedicated to the advancement of electronic government within the states. The NECCC is composed of NASIRE (a group representing the chief information officers of the states), the National Association of State Auditors, Comptrollers and Treasurers (NASACT), the National Association of State Procurement Officers (NASPO) and the National Association of Secretaries of State (NASS). In addition to these voting members, other governmental and private organizations participate in an advisory capacity. These associations include the National Governors Association (NGA), the National Association of State Chief Administrators (NASCA), the Information Technology Association of America (ITAA) and the National Automated Clearing House Association (NACHA). The ITAA and the NACHA specifically represent private information technology companies and the financial services and technology industries.

NECCC Audit Guidance Committee

Chair
Nancy Rainosek, TX
State Auditor's Office

Co-chair
Joe Moore, AZ
Office of the Auditor General

Members

Michael Billo, PA
Department of the Auditor General

Frank Bowker, NJ
Office of Legislative Services

Bob Dacey
U.S. General Accounting Office

Dale Dillon, UT
Office of the State Auditor

Mike Farrar, NY
Office of the State Comptroller

Kelton Green, TX
State Auditor's Office

Jon Ingram, FL
Office of the Auditor General

Carol Langelier
U.S. General Accounting Office

Mark Matlock, PA
Office of the Budget

Terri Morrow, PA
Department of the Auditor General

Sherrill Norman, FL
Office of the Auditor General

Jennifer Schreck, VA
Auditor of Public Accounts

Martin Vernon, NC
Office of the State Auditor

Sharron Walker, OR
Secretary of State, Audits Division

For More Information Contact:
Brandon W. Lenoir, Director
NECCC
202-624-5451 or blenoir@nasact.org
or visit http://ec3.org

TABLE OF CONTENTS

Page

A. Introduction 4

B. E-government Critical Business Issues

Leadership/Governance 5
Privacy 6
Security 7
Technology 7
Legal Readiness 8
Customer Readiness and Accessibility 8
Applications 9
Competencies 10

Appendices

C. E-government-Related Definitions 11
D. Electronic Service Delivery Targets 13
E. Vendor Approaches to a Self-Funded Portal Project of a Particular State Government 14
F. Georgia Technology Authority SB 465 Summary 15

Advances in technology have significantly affected the way we live, communicate, and do business. The World Wide Web (web) allows people to use their computers to purchase goods and services without ever leaving their homes. For the first time since computers entered the workplace, organizations are achieving documented cost-savings due primarily to Internet technologies.

Advances in technology are also changing the way governments do business with citizens. Today's progressive governments are introducing electronic methods for delivering services (such as renewing driver's licenses and vehicle registrations), commonly referred to as e-government. (Appendix A contains definitions of common terms used in the new electronic environment.) This paper describes the critical business issues and best practices that decision-makers, managers, and auditors should be aware of as their governments transform themselves into e-governments.

When doing business with traditional governments, a citizen is expected to know where to go to get the services they need. The details of their transaction stay within the agency and the agency's information systems. This causes a duplication of data and systems as the citizen conducts business with other agencies. It also makes it difficult for government leaders to get high-level information about their organizations. (Figure 1 depicts a typical citizen's transactions with traditional government.)

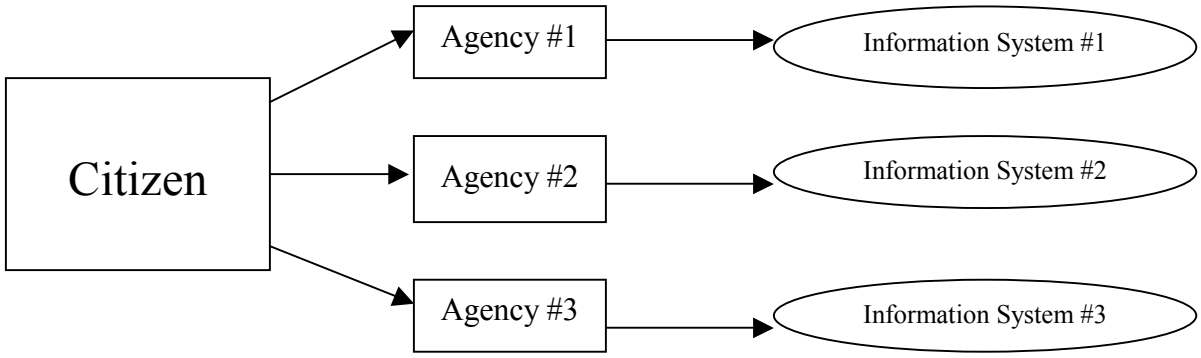


Figure 1

One goal of an e-government initiative is to provide a site on the Internet's World Wide Web where citizens can access government services at a reduced cost, regardless of which agency actually provides the service. To be successful, this site should be designed from the citizen's point of view, making services easy to locate and use. (Figure 2 depicts the ideal citizen interaction with e-government.)

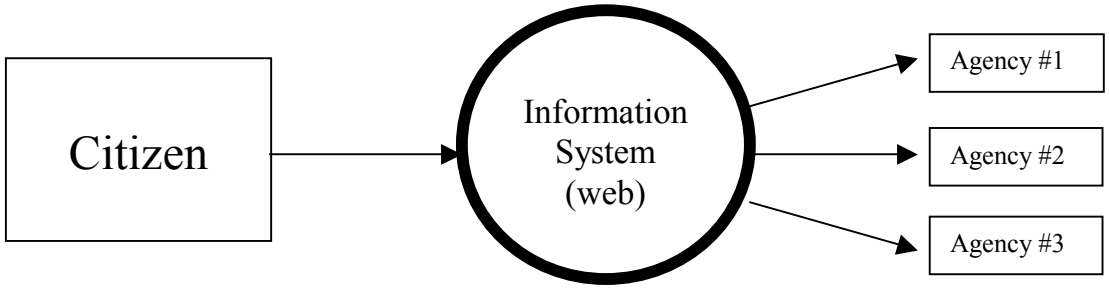


Figure 2

A well-designed e-government benefits all citizens, even those who continue to do business through traditional means. By providing services to people through electronic methods, those citizens who choose traditional methods will encounter shorter lines as they transact business with their governments. In automating routine services, government employees can spend their time serving citizens with special needs. Governments will provide more individualized services at less cost to the taxpayers. This means everybody wins.

And it translates to governments saving money. The Institute for Electronic Government describes the range of possible cost-savings by delivering services online in a 1999 white paper. "Depending upon the service, the population required to use that service, and other variables, early studies indicate governments are saving up to 70 percent by moving services online compared to the cost of providing the same services over the counter." [1] For example, Alaska's citizens can receive new registration tags in three to five days instead of four to six weeks; transaction costs have been reduced from $7.74 to less than a dollar; and the average time to renew vehicle registration has been reduced to less than 100 seconds. [2]

Furthermore, e-government systems give decentralized governments an opportunity to develop enterprise-wide information models. This means that top government decision-makers finally have a way to effectively get the information they need to oversee their large governments.

To realize the benefits that can be achieved through e-government, governments must be willing to change their traditional structures and business processes. These changes may be accomplished through legislation to reorganize the traditional government model, modification of existing statutory and regulatory requirements, and through strong IT leadership and policy.

Leadership/Governance

Visionary leadership, joined with thoughtful planning and monitoring, can make e-government a useful vehicle for government services and information. Ideally, government leaders will establish a central authority (Chief Information Officer [CIO] and/or a governance council) with responsibility for setting a unified direction for developing e-government. This responsibility includes setting targets for service delivery, setting policies for operation, and determining funding methods. An e-government initiative without a unified direction increases the risk of failures such as incompatible systems, poor interoperability, duplicate systems, and ineffective security. In other word, somebody needs to be in charge of and held accountable for:

- **Effective plans that provide a road map for the future.** A CIO or governance council can ensure that applications that meet the highest public need are implemented, versus the programs of agencies rich in funding. They can also ensure that high-level government information is readily available for their government's decision-makers. They can make decisions about the shared data of the entire government, as opposed to different agencies negotiating such decisions, costing additional time and effort in the transformation to e-government.
- **Establishing targets, measuring results, and holding agencies accountable for meeting goals.** Governments need strong central leadership to establish targets, measure results, and hold agencies accountable for meeting goals. (See Appendix B for an explanation of Electronic Service Delivery Targets.) Agencies should determine how they can better meet customer needs (in terms of outcomes)

[1] *The Quest for Electronic Government: A Defining Vision*, by Janet Caldow. Institute for Electronic Government IBM Corporation, July 1999
[2] *Alaska's On-line Webmart Services Included in the Smithsonian's National Museum of American History*, http://www.state.ak.us/itg/news/sagasmith.html

and then seek the technology to do this, rather than taking an approach of 'lets do it because we can'. Service levels should be defined so that monitoring can evaluate whether the means for providing goods or services electronically are effective. In other words, is it beneficial to automate the process?

- **Ensuring that processes are reengineered to take advantage of potential cost-savings.** It seems that some government agencies have decided against re-engineering, yet that is where the largest savings appear to be possible. High level decision-makers should be aware of the potential cost-savings and hold government agencies accountable for achieving the results enabled by new technologies. The central leader should also ensure that agencies re-engineer processes, not merely move them as they exist today to the Internet. One big issue is how the changes from re-engineering are managed from a people perspective. Naturally, many of the gains from re-engineering come from staff - either redeployment or redundancy/retrenchment. It is common for there to be a lot of resentment and opposition to such change and it can be difficult to manage. Often there are also legal and industrial impediments. The costs of change management, including retraining and retrenchment costs, need to be factored in and the risk of non-cooperation needs to be considered.
- **Recommending adequate funding methods for initial development as well as ongoing maintenance and operations.** Governments continually grapple with how to fund their e-government efforts. The central authority should ensure that the e-government funding method aligns with citizen expectations. Governments must take a long-term view of the potential profits from e-government web sites and ensure that contracts do not give vendors an unreasonable return on their investments. (An example of methods proposed for one state's self-funded portal is detailed in Appendix C.)

An example of a unified e-government effort can be found in Georgia, which recently passed a law establishing a governance council and CIO to oversee its technology initiatives. The law also establishes roles for Georgia's Technology Authority (GTA) including responsibility for management issues and the internal audit of agency operations by the GTA. It is important that the central authority have the ability to assess agency compliance with e-government directives. It is equally important that the government's independent external auditor assess e-government programs. This gives government leaders assurance that the overall e-government initiative is effectively carried out. (Appendix D contains a summary of Georgia Senate Bill 465, which went into effect on July 1, 2000.)

Privacy

Governments collect information on individuals' identity and finances. Governments also collect certain information electronically from private companies. This includes statutorily required corporate filing information, tax information, and regulatory information.

Governments need to protect citizens' privacy or the public may lose confidence in e-government. Even before the advent of e-government, some government entities made a practice of selling information about citizens. For example, selected information from driver's license or vehicle registration rolls has historically been sold to companies for use in marketing. This practice could grow dramatically as greater amounts of information are collected and linked electronically by governments.

A comprehensive privacy policy should specify citizens' rights to privacy and require that personal data be collected and processed only for legitimate purposes. Two types of information may be collected: the data involuntarily provided by accessing a web page and the data voluntarily provided to complete a transaction. Privacy policies should address the collection and handling of both types, including specifically addressing the practice of selling or sharing citizen information.

Federal and state laws and regulations currently mandate the confidentiality of certain information. In light of the advent of e-government, these requirements may need to be re-examined and enhanced. Governments should only retain citizen information long enough to fulfill the official business purpose.

Security

As citizens and businesses submit more information to governments over the Internet, the risk of it being stolen or misused increases. A serious concern is the theft of a citizen's identity, which can result in financial loss to the citizen. Governments should also understand and lessen the risk of inappropriate disclosure of proprietary business information that they collect from companies. User IDs, passwords, credit card numbers, bank account numbers, and other such data are transmitted over the Internet and stored electronically in e-government applications. Should theft occur, the government entity holding the information could be subject to litigation as well as embarrassment.

Therefore, an effective security system — one designed to protect data where it is stored and during transmission from citizen or business to government — is essential to e-government. It protects the citizens, businesses and the government by:

- Safeguarding assets and sensitive information from loss, misuse, inaccuracies, or alteration.
- Preventing interruptions in service delivery.
- Validating the identities of the parties involved in any transaction or data exchange.

These objectives are largely accomplished through the use of security technology, such as digital signatures, encryption, and firewalls. However, due to rapid changes in technology, these security measures must be reviewed, monitored, and tested regularly. In addition, citizens must be educated about the necessity of security measures, such as private passwords, for their own protection.

Technology

As computer systems become more and more interconnected, controlled planning, design, development, and implementation are key factors in creating systems that work with other systems. Standards to monitor development and to ensure compatible communications are essential. The hardware and software that build and connect these systems must accommodate rapid growth and provide for continued interoperability.

Systems must be designed to provide a user-friendly, single point of entry that an average citizen can access. Service levels must be adequate to attract users and demonstrate benefits of use. Regardless of the technology used, sufficient testing of system interfaces is crucial to effective operability. System design must also address policies for data retention so that any discrepancies or customer complaints can be resolved.

Given the vast amount of technology available, governments should be mindful of standard platforms and tools that have been proven reliable. Technical requirements for creating effective networks, Internet and Intranet connectivity, must be carefully planned.

Technology will continue to advance rapidly and governments must face the challenges of e-government to thrive in the 21st century. With this in mind, systems should be developed with the flexibility to

accommodate changes in technology and provide a continued ability to communicate in the modern world.

Legal Readiness

An effective legal framework ensures that governments have the opportunity to keep pace with the new era of global communication and efficiently provide citizens with valuable services. This framework should identify and address legal obstacles to e-government. Legal obstacles may include the differences that exist between traditional data collection requirements (that is, sharing of information collected by and provided to various government agencies) and the ease of electronically collecting and sharing data.

Legislative revisions may be required, as current laws, rules, and regulations may not recognize the legality of electronic documents and processes. For example, legislation should ensure that electronic authorizations, contracts and signatures have the same legal effect as those done on paper. (However, due to the nature of technology, giving them the same legal effect may change or even eliminate the traditional ways these items are completed, such as the notarizing of a document.) Additionally, governments may consider the required quorum at meetings to be met through the electronic participation of officials rather than by the officials' physical presence.

Ideally, a legal framework that allows for the implementation of e-government processes and services will:

- Preserve basic public policy goals, such as privacy and security, retention, and public access to information.
- Provide the statutory basis of, authority for, and regulations related to the government processes and services that may be supplied electronically.
- Assign responsibility for and ownership rights to the data provided and accumulated electronically.
- Address the sharing of data collected by one government agency with other government agencies that require the same information.
- Clearly define jurisdictional responsibilities related to intergovernmental transactions and business to government transactions.
- Provide a mechanism by which legal requirements are recognized and enforced.
- Provide a basis for the establishment of fees related to electronic processes and services.
- Identify the records that should be maintained, the period of retention, and the required storage media.
- Not be technology-specific or favor one form of service delivery (traditional or electronic).
- Minimize costs and the potential for litigation.

To adapt to the electronic environment, governments need to establish a legal framework that treats electronic processes and traditional processes equally.

Customer Readiness and Accessibility

For policy makers, a key concern has always been the impact of new developments on the public and whether all sections of society are benefiting equally from any new system. This concern is even greater with the use of technology to provide services because accessibility to those services is not the same for everyone. For example,

- People who can not easily afford or access a computer will not receive the benefits of e-government;
- People who are blind or visually impaired may not be able to read a web site;
- People who do not speak or read English may not be able to access services;
- People in rural areas and inner city neighborhoods may have less access to the Internet than others;
- People who have never used computers may simply be reluctant to use the new technology;
- People without bank accounts or credit cards may be prohibited from using the technology if there are no other methods to pay for the services;
- People may not trust the government to use the information they provide only as intended.

As an example, a single parent of two children, struggling to make ends meet on a salary of less than $15,000 a year can barely afford apartment rent, groceries, utilities and telephone payments in many parts of the country. Trying to save enough money to purchase a computer, and then pay access fees to connect to the Internet is out of the question.

This digital divide - the gap between those households that have access to the Internet and data services and those that do not - may be addressed by placing computers in locations such as grocery stores, post offices, libraries, and shopping malls. However, this may be a temporary solution at best, since the location is also an issue: people may not be comfortable entering personal information in computers that are in public locations. It is also critical to address the security over the data collected to help instill the confidence that government can be trusted to protect the individual's privacy.

Additionally, government officials need to keep in mind that traditional service methods need to continue, at least in the short term. Government is different than private industry, since the public does not have the choice of dealing with government providers. For example, people cannot shop around to purchase their motor vehicle registrations from any organization they want. They must deal with their state or local government to get this registration. Because of this, government must provide the choice in how the interaction occurs, whether that choice is face to face at a traditional counter service or using technology over the Internet.

Furthermore, when developing applications, new technologies that enable adequate access to web content for individuals with disabilities or other special requirements need to be considered. Appropriate and customized training may be necessary to increase people's comfort level in using computers. Alternative payment methods, such as pre-paid benefit or cash cards may be required to allow more people to access the services they need.

Applications

Any application development initiative needs user sponsors to ensure data is gathered and processed correctly. Developing applications that span government agencies and policies supporting those applications makes the assignment of responsibility even more critical, especially since these applications represent the face of government to the citizen. In this environment specific issues arise such as:

- Who owns and maintains the data collected for a variety of government organizations, particularly if the data is stored in separate databases and then transferred to the central site for display to the public?
- Who ensures data is correct, and what processes are used to ensure that data in back-office systems is changed when changes occur at the central site?

- How does government integrate data of various agencies, and who "makes the call" when systems have to change to make the information consistent? Who decides on security levels and access levels when agencies disagree?
- Who ensures that computer programs are tested and processing data accurately?

Without the assignment of responsibility, the assurance that information gathered or distributed is correct, reliable, and from a valid/verified source is at risk.

Competencies

Once the leadership, technology, and policies are in place, the final piece of the initiative lies with the human resources supporting e-government. The competency of the individuals developing, implementing, and supporting technology drives the effectiveness and efficiency that can be achieved through e-government. Without the appropriate resources dedicated to the electronic government effort, the benefits available through technology cannot be fully realized, and the technology may fail.

Many organizations and governments have experienced the harsh reality of system development initiatives that had to be abandoned due to poor project management, improper planning, and insufficient resources. For all of the reasons mentioned here and in previous sections, the dedication of appropriate human resources is critical to any electronic government initiative. And, maintaining the knowledge, skills and abilities of that workforce is imperative. This requires the ongoing recruitment of qualified employees, the continued training of current employees to match technology changes or the adoption of technology within available competencies, and the consideration of consultants or contracted employees and the competencies they offer.

C. Appendix A – E-government-Related Definitions

- *Authentication* – Authentication is the means by which assurance of the identity of parties to a transaction is established. The authentication concern is: How do I know this web site is actually the agency that it purports to be?
- *Confidentiality* – Confidentiality is the assurance that no one is able to eavesdrop on the transaction in progress. The confidentially concern is: How do I know no one is listening (in on my transaction)?
- *Digital Divide* – The "digital divide" is the gap in opportunities experienced by those with limited accessibility to technology especially, the Internet. This includes accessibility limitations in the following categories:
- Social Issues (need to talk to a person, etc.)
- Cultural Issues (language barriers, etc.)
- Disability Issues (ADA, etc.)
- Economic Issues (access to technology devices)
- Learning Issues (marketing, overcoming unfamiliarity, changing habits)
- *Digital Society* – A society or community that is well advanced in the adoption and integration of digital technology into daily life at home, work and play. A Digital Society is one that is advanced in the adoption of the New Economy.
- *E-Business* - The transformation of internal and external business processes toward customer-centricity based upon service delivery opportunities offered by new communications technologies (such as Web-based technologies) to better fulfill the purposes of private entities to provide efficiency and effectiveness as well as profitability.
- *E-Commerce* - The use of communications technologies (such as Web-based technologies) for the conduct of business and service delivery transactions while leaving internal or external business processes substantially unchanged.
- *E-government* - The transformation of internal and external business processes toward customer-centricity based upon service delivery opportunities offered by new communications technologies (such as Web-based technologies) to better fulfill the purposes of government to provide efficiency and effectiveness as well as fairness and equitability.
- *E-government Strategic Plan* – A written plan that answers the question, "What could or should we do to transform our organization to be customer-centric in service delivery?"
- *E-government Implementation Plan* – A written plan that answers the question, "What will we do to transform our organization to be customer-centric in service delivery?"
- *IT Governance* – Cross-jurisdictional organizational structure that provides a decision-making process for the determination of the services, architecture, standards and policies for the organizations information technology. (Determination of who does what and how it gets decided as to who does what)

- *IT Infrastructure* – The systems and network hardware and software that supports applications. IT infrastructure includes servers, hubs, routers, switches, cabling, desktop, lap and handheld devices.
- *Privacy* – The assurance that information provided for a specific transaction will not be used by the recipient for purposes not authorized by the provider. The privacy concerns is: How do I know what you are going to do with my data?
- *Readiness* - Readiness is the degree of preparedness to accomplish an endeavor. E-government Readiness is the degree to which a government is prepared to provide its information and services through multiple channels including the Internet toward customer centricity. Digital Society Readiness is the degree to which a community is prepared to participate in the e-conomy.
- *Security* – Security is protection from intended and unintended breaches that would result in the loss or dissemination of data.

D. Appendix B - Electronic Service Delivery Targets

One tool widely viewed as a best practice is the establishment of electronic service delivery (ESD) targets. Countries leading in the transformation to e-government have established specific ESD targets. For example, Australia has established the target of having all appropriate federal government services delivered via the Internet by 2001. The United Kingdom set a target of 100 percent of government services carried out electronically by 2005.

A review of the top ten state e-government sites (according to the January 2000 rating by the Center for Digital Government) revealed that most state governments have not published targets. States with published ESD targets had numerous ways of conveying their goals, the most specific being laid out in a bill by the Governor of Maryland:

> The Maryland bill requires all units of the executive branch, with the exception of public institutions of higher education, to have: (1) 50% of their public information and services available over the Internet by 2002; (2) 65% of their public information and services available over the Internet by 2003; and (3) 80% of their public information and services available over the Internet by 2004. Each unit must also provide the Secretary of the Department of Budget and Management with an annual project plan outlining the status of their efforts to comply with the time frames.[3]

[3] From "Maryland's Technology Agenda," http://www.techmd.state.md.us/techagenda2000.htm

E. Appendix C - Vendor Approaches to a Self-Funded Portal Project of a Particular State Government

Vendor	Return to State	Projected Percentages Over 5 Years	Returns Based on Revenues of $50 Million (stated in millions)
1	State receives 35% of net profit in the form of new services performed by the vendor.	Portal Expense 40% Vendor 39% State 21%	$20.2 $19.3 $10.4
2	Additions to the portal would be based on a business case, and funded through cost savings to state agencies.	Portal Expense 15% Vendor 0% State 85% (vendor revenue is included in portal expense)	$7.5 0 $42.5
3	State receives 10% of gross revenues generated by portal. State and vendor share net revenue equally after all vendor expenses are recovered.	Portal Expense 49% Vendor 16% State 35%	$24.6 $7.7 $17.7
4	State receives 4 – 6% of gross revenues generated by the portal.	Portal Expense 45% Vendor 53% State 2%	$22.4 $26.5 $1.1

F. Appendix D - Georgia Technology Authority SB 465 Summary

Section 1
This section is a summary of the bill that establishes the Georgia Technology Authority (GTA), which is the successor in interest to the GeorgiaNet Authority. This section also charges the GTA with the development of a single Internet site for the General Assembly.

Section 2
This section relates to the keeping of records of applications for licenses and information on licensees.

Sections 3, 4 and 5
These sections list the various deletions to existing laws, which established certain responsibilities for the Department of Administrative Services (DOAS) and now transfers them to the GTA.

- Electronic Data Processing-Printing Committee
- The Telecommunications Consolidation Act of 1973
- The Public Safety Radio Services Act of 1975

Section 6
This section refers to the Georgia Distance Learning and Telemedicine Act of 1992. Responsibilities under this act are transferred from DOAS to GTA.

Section 7
This section makes GTA the successor to the GeorgiaNet Authority. In general terms, it also describes the purpose of GTA as follows:

- The purpose of the GTA shall be to provide for procurement of technology resources, technology enterprise management, and technology portfolio management as defined in this chapter, as well as the centralized marketing, provision, sale, and leasing, or execution of license agreements for access on line or in volume, of certain public information maintained in electronic format to the public, on such terms and conditions as may be determined to be in the best interest of the state in light of the factors listed in the code.

Section 8
This section describes the GTA governing board, which shall consist of 11 voting members appointed as follows:

- Two members appointed by the Lieutenant Governor.
- Two members appointed by the Speaker of the House of Representatives.
- Seven members appointed by the Governor.
- The Governor shall designate a member of the GTA to serve as chairperson.
- All of the voting members shall be individuals employed in the private sector who have experience in technology issues concerning large public or private organizations or entities.
- In addition, there shall be one nonvoting ex officio member who shall be appointed by and serve at the pleasure of the Chief Justice of the Supreme Court.

Section 9
This section relates to the administration of the GTA. For administrative purposes, the GTA will be assigned to DOAS, and the Attorney General will provide legal services.

Section 10
This section defines the powers of GTA, which include the following items:

- Make and execute contracts, lease agreements, and other instruments.

- Acquire and dispose of real or personal property of every kind and character.
- To apply for and to accept any gifts or grants or loan guarantees or loans of funds or property or financial or other aid in any form from the federal government or any agency or instrumentality, or from the state or any agency or instrumentality, or from any other sources.
- To contract with state agencies or any local government for the use by the GTA of any property, facilities, or services of the state or any such state agency or local government or for the use by any state agency or local government of any facilities or services of the GTA.
- To fix and collect fees and charges for data, media, and incidental services.
- To deposit or invest funds.
- To establish standards for agencies to submit information technology plans to the GTA.
- To provide and approve a technology plan to include strategic planning and direction for technology acquisition, deployment development, and obsolescence management as well as a communications plan to manage costs for voice, video, data, and messaging services for all agencies.
- To set technology policy for all agencies except those under the authority, direction, or control of the General Assembly or statewide elected officials other than the Governor.
- To prescribe procedures for the procurement of technology resources for agencies.
- To provide oversight and program management for all technology resources for projects exceeding a cumulative investment of $1 million to accomplish goals of technology portfolio management.
- To require agencies to submit periodic reports.
- To prepare fiscal impact statements relating to necessary modifications and development of technology to support policies required by proposed legislation.
- To establish architecture for state technology infrastructure to promote efficient use of resources and to promote economic development.
- To provide processes and systems for timely and fiscally prudent management of the state's financial resources.
- To establish advisory committees including a standing advisory committee composed of representatives from agencies, which shall make recommendations to the GTA concerning policies, standards, and architecture.
- To coordinate with agencies, the legislative and judicial branches of government, and the Board of Regents of the University System of Georgia regarding technology policy.
- To coordinate with local and federal governments to achieve the goals of the GTA.
- To identify and pursue alternative funding approaches.
- To establish technology security standards and services to be used by all agencies.
- To conduct technology audits of all agencies.
- To facilitate and encourage the conduct of business on the Internet.
- To expand and establish policies necessary to ensure the legal authority and integrity of electronic documents.
- To provide and approve as part of the state technology plan an implementation plan and subsequent policies and goals designed to increase the use of telecommuting among state employees.
- To create a center for innovation to create applications of technology that will yield positive, measurable benefits to the state.
- To establish benchmarks for contracts requiring approval by the board.
- To canvass sources of supply and to contract for the lease, rental, purchase, or other acquisition of all technology resource related supplies, materials, services, and equipment required by the state government or any of its agencies under competitive bidding or to authorize any agency to purchase or contract for technology.
- To establish and enforce standard specifications which shall apply to all technology and technology resource related supplies, materials, and equipment purchased or to be purchased for the use of state

government or any of its agencies, which specifications shall be based on and consistent with industry accepted open network architecture standards.
- To establish processes, specifications, and standards for procurement, which shall apply to all technology to be purchased, licensed, or leased by any agency.

Section 11
This section discusses the role of the Chief Information Officer (CIO), who serves as executive director of the GTA. The CIO shall be both appointed and removed by a vote of a majority of the full Board membership.
Among the powers of the CIO are the following:
- Supervise, direct, account for, organize, plan, administer, and execute the functions required of the CIO by the GTA.
- Provide assistance to agency heads in evaluating information officer performance for each agency and in selection of candidates for such positions.
- Establish performance management standards, approved by the Board regarding success of projects, agency technology performance, and authority performance.
- Submit an annual and a three-year technology plan, updated annually, and an annual budget for approval and adoption by the Board.
- Review periodic reports submitted by agencies.
- Hire officers, agents, and employees, prescribe their duties and qualifications, and perform such other duties as may be prescribed by the GTA. Officers, agents, and employees shall serve at the pleasure of the executive director. The executive director and other employees of the GTA shall be considered state employees in the unclassified service of the State Merit System of Personnel Administration.
- Contract for the services of individuals or organizations not employed fulltime by the GTA who or which are engaged primarily in the rendition of personal services rather than the sale of goods or merchandise.

Section 12
This section discusses the role of the GTA and the CIO and includes the following:
- The GTA is authorized and directed to establish a technology empowerment fund to be administered by the GTA.
- The CIO is authorized to identify and select individual projects, initiatives and systems to improve service delivery to be funded through the technology empowerment fund.
- Each project or initiative developed and supported from the technology empowerment fund shall employ technology that is compatible with the architecture and standards established by the GTA.
- A steering committee shall advise and consult with the CIO regarding initiatives to receive funding from the technology empowerment fund and shall receive quarterly reports from the CIO as to the status of funded projects.
- All agencies shall contact through the GTA for any technology resource purchase of such agency exceeding $100,000; provided, however, that the provisions of the code section shall not have application to fulltime state personnel tasked with the planning, implementation, and support of technology. The GTA shall be authorized to act as the agent for any agency for such purposes. No agency shall divide purchases so as to avoid the thresholds provided for in the code section.
- Any agency whose direct or indirect appropriation for technology resources is less than $50,000 shall not be required to contract through the GTA for the purchase of such technology resources.
- No section in the code shall exempt any technology resource purchase from the technical standards and specifications established by the GTA unless specifically provided by action of the GTA, provided, however, that technical standards established by the GTA shall not conflict with mandated federal technical standards or requirements associated with the state administration of federally funded programs.

- Except as otherwise provided, contracts shall be awarded by soliciting competitive sealed proposals or competitive sealed bids.
- The GTA is authorized to promulgate rules and regulations to implement the procedures of the code or by rule and regulation to implement alternative purchasing procedures advantageous to the state.
- Perspective suppliers may be prequalified for particular types of supplies, services, goods, materials, and equipment at the discretion of the GTA.
- If needed supplies, materials, or equipment can reasonably be expected to be acquired for less than $2,500 and are not available on state contracts or through statutorily required sources, the purchase may be effectuated without competitive bidding.
- Neither the executive director nor any employee of the GTA shall be financially interested or have any personal beneficial interest either directly or indirectly in the purchase of or contract for any materials, equipment, or supplies, nor in any such firm, corporation, partnership, or association furnishing any such supplies, materials, or equipment to agencies or the GTA.
- The executive director shall submit to the director of the Office of Planning and Budget and the state auditor on a quarterly basis a report of all activity regarding technology and technology resources for each agency and the GTA.
- The Governor shall have the authority to transfer the technology resources as provided in the code of all state agencies, except those under the authority, direction, or control of the General Assembly or statewide elected officials other than the Governor, to the GTA. This code section shall be implemented by executive order of the Governor, and the Governor shall have the authority to implement this code section in whole or in part, in phases or stages, or in any manner or sequence which he or she may deem appropriate. In making such transfer, the Governor shall assure that the transfer shall not interrupt such agency's services.
- The GTA, the Office of Planning and Budget, and the state auditor shall jointly develop a system for budgeting and accounting of expenditures for technology resources.
- The GTA shall adopt procedures to ensure that the GTA and agencies do not acquire, reproduce, distribute, or transmit computer software in violation of United States copyright laws and applicable licensing restrictions.
- The GTA shall establish procedures to ensure that each agency has present on its computers and uses only computer software that complies with United States copyright laws and applicable licensing restrictions.

Section 13
This section deals with deletions to the Information Technology Policy Act of 1995 and makes the GTA the successor in interest to the Georgia Information Technology Policy Council.

Section 14
This section authorizes the establishment of pilot projects, which shall be approved by the GTA. Also, the Electronic Commerce Study Committee shall have 12 members, and the GTA CIO shall serve as a member of the committee. The Electronic Commerce Study Committee shall be terminated on December 31, 2002.

Section 15
This section says that the Act becomes effective on July 1, 2000.

Section 16
This section says that all laws and parts of laws that are in conflict with this Act are repealed.