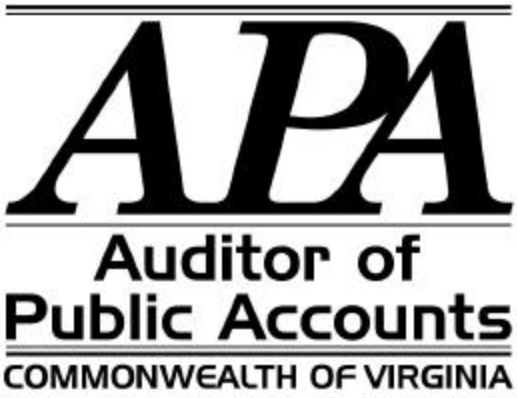
A STUDY OF ELECTRONIC COMMERCE:
AUDITABILITY AND OBSTACLES

REPORT ON
SENATE JOINT RESOLUTION 72
NOVEMBER 2000



We have determined that audits of public accounts can satisfactorily occur in an environment using electronic procurements, contracts, and transactions.

We identified several statutory and regulatory obstacles that are contained within this report. The success of e-commerce relies on addressing these obstacles. Some of the recommendations are as follows:

- The Secretary of Technology must establish information technology guidelines and standards for agencies to follow when implementing e-commerce.

- The General Assembly should re-evaluate the assessing of fees when citizens pay taxes, licenses, and other revenues by credit card, particularly where agencies can demonstrate that the use of credit cards can reduce administrative costs.

- The General Assembly may wish to determine if the Virginia Freedom of Information Act should provide additional protection of credit card information.

- The Virginia Public Procurement Act provides policy statements, such as encouraging competition and facilitating small business participation. The General Assembly should determine the most appropriate action to take concerning these policies in light of e-commerce.

- The Departments of General Services and Accounts should update their manuals to allow for the use of e-commerce.

- Agencies should recognize the need for continuous training of managers and internal auditors on e-commerce and the changes in business processes and internal controls that can result.

- To successfully implement the Commonwealth's e-procurement solution, there is a need to: develop data integrity, authentication and non-repudiation controls; mandate that agencies transfer purchase data to the central data warehouse; and include EDI as a payment method within the e-procurement system.

Senate Joint Resolution 72 required our office to study electronic commerce to:

- Determine whether audits of public accounts can be satisfactorily conducted using electronic procurements, contracts and transactions; and,

- Identify any statutory or regulatory barriers or obstacles, which may prevent the implementation of electronic contracting and electronic procurement processes that are envisioned for the Commonwealth.

Table of Contents

Commonwealth of Virginia

Walter J. Kucharski, Auditor

Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

November 6, 2000

The Honorable James S. Gilmore, III
Governor of Virginia
State Capitol
Richmond, Virginia

Members of the Virginia General Assembly
General Assembly Building
Richmond, Virginia

We have completed our study of electronic commerce as directed by Senate Joint Resolution 72 of the 2000 General Assembly and are pleased to submit our report entitled "A Study of Electronic Commerce: Auditability and Obstacles."

Scope

To conduct this review and determine if barriers or obstacles exist, we developed a working definition of e-commerce by examining numerous sources of information. Further, we researched e-commerce initiatives of other states and the federal government. While other states use e-commerce for citizens to access government services, the Commonwealth is one of only a handful of states preparing to use e-commerce to connect government to business for the purpose of purchasing goods and services.

Results

We have determined that audits of public accounts can satisfactorily occur in an environment using electronic procurements, contracts, and transactions.

We have identified several statutory and regulatory obstacles and outline them within this report. The success of electronic commerce relies on addressing these obstacles.

Exit Conference

We discussed this report with agency directors from the Departments of Accounts and General Services and the Secretary of Technology and his staff on November 6, 2000.

AUDITOR OF PUBLIC ACCOUNTS

JBS:kva
kva:61

Introduction

Senate Joint Resolution 72 directed the Auditor of Public Accounts to review the auditability of e-commerce and any statutory or regulatory barriers or obstacles to its implementation. In conducting this review, we found that no agency, group or source shares a consistent concept or vision of what e-commerce is, or what it should be.

To conduct this review and determine if barriers or obstacles exist, we developed a working definition of e-commerce by examining numerous sources of information. We believe the following definition encompasses most of the current concepts and provides a broad definition of e-commerce.

Definition of Electronic Commerce:

Electronic commerce is the conduct of business and activities in a paperless environment. It includes those transactions that support revenue generation, such as offering services and customer support as well as the procurement of and payment for goods, services, information and investments either over the Internet or across private networks using EDI, E-mail, EFT, or other similar technologies. E-commerce builds on traditional commerce by adding the flexibilities offered by electronic networks. It enables new forms of business as well as new ways of doing business.

We began our study by researching e-commerce initiatives of other states and the federal government. While other states use e-commerce for citizens to access government services, the Commonwealth is one of only a handful of states preparing to use e-commerce to connect government to business for the purpose of purchasing goods and services.

Traditional vs. E-Commerce Model

To contrast current government operations with those possible with e-commerce, we have prepared some examples of how current operations would change in an e-commerce environment. Below we discuss citizen payments and some purchasing examples.

Governments collect revenues and make purchases to support government services. Revenue sources include taxes, registrations, licenses, permits, fees, and fines. Purchases range from buildings and professional services to office equipment and paper clips.

Citizen Payments

Governmental agencies responsible for revenue collection typically accept cash, check or credit card payments in person or by mail. Accompanying the payment is a hard copy form completed by the citizen containing information critical to the transaction. The agency must then enter this information into a database, which eventually flows into an accounting system.

Some governments are beginning to allow citizens to conduct these transactions over the Internet. In these cases, citizens pay by credit card and complete an electronic form, which integrates automatically into the government's information system, eliminating the need for data entry. This process can reduce the need for clerical staff to perform data entry and allow them to focus on other initiatives, such as improving customer service. The process can also improve cash flow by decreasing the opportunity for bad debts.

The citizens using this method also realize benefits, primarily convenience. They can save time by having immediate access to government as well as having around the clock access to services.

Purchases

When making purchases, governments have established specific guidelines to encourage competition and obtain the best product at the fairest price. Government purchases begin with an employee requesting an item, including its specifications. This request passes through an approval process depending on the cost of the item. The request then moves to the purchasing department where a purchasing officer follows the purchasing guidelines, which may include searching state contracts and vendor catalogs as well as contacting vendors directly by phone. Once the purchasing officer selects a supplier, he submits a purchase order.

Upon receiving the order, the vendor verifies credit, checks the warehouse for inventory, ships the item to the appropriate location, and bills the agency. When the government receives the item and the invoice, the accounts payable department processes a check to pay the vendor.

When purchasing small quantities using e-commerce, the employee goes to the vendor's web site and selects an item matching his needs from an on-line catalog. The employee uses e-mail to digitally request a manager approval. Once approved, the manager forwards the e-mail request to the purchasing department and the purchasing department sends an electronic purchase order to the vendor. The purchasing department could make payment using a credit card.

When the purchase requires competition or the government wishes to establish large on-going contracts, the purchasing officer has many purchasing guidelines to follow depending on the dollar value involved. These guidelines can range from searching multiple vendor web sites to competitive bidding, with the overall goal of obtaining the best value.

The result of this process could be the establishment of a partnership agreement between the agency and the vendor that allows for ongoing purchasing and payment of goods and services. These partnership arrangements may take many forms. For example, the partnership may be a drug supplier providing a computer and software for a pharmacy to

track and set critical inventory levels. The drug supplier could directly contact the computer and periodically, based on inventory level and other information, restock the pharmacy. The local pharmacist would then enter the receipt of the drugs and authorize on-line payment for the order. This authorization would update the accounting system before making payment.

In another circumstance, the vendor could electronically receive an order, automatically insert the order into a database, check inventory and credit status, pass the request directly to the warehouse, and create an invoice. The vendor would then electronically bill the agency and the accounts payable department would electronically match the invoice with the receiving report. Once the system matches the information, the data updates the accounting system, which electronically pays the vendor.

General E-Commerce Practices

General e-commerce practices have emerged to allow parties to effectively communicate and conduct business over the Internet. Websites provide the starting point for implementing e-commerce and often include company and product information, search engines, links to other resources, and electronic forms that mirror traditional paper forms.

E-commerce depends on network infrastructures, including the Internet and private networks, to move information. In an effort to standardize these networks, the International Standards Organization created a seven-layer model that defines basic network functions. This model defines protocol specifications for how networks exchange data. As long as these specifications are followed, new and better functionality can be substituted without affecting the network's behavior. Some standard protocols include TCP/IP, FTP, HTTP, and HTML.

The revenue collection and payment sides are the most fluid and fast changing part of e-commerce, involving the use of credit cards, EDI, digital cash, and electronic checks. However, no matter what changes are made, there are expectations involving confidentiality, integrity, authentication, and authorization in dealing with financial transactions on which people have come to depend.

For example, in a traditional financial transaction, purchasers expect confidentiality in that vendors will only disclose critical information such as credit card and bank account numbers to those who need to know it. Purchasers also have integrity expectations, such that vendors will not inappropriately alter the purchase amount. Vendors may require authentication that the purchaser is really who they claim to be and verify this by requesting proper identification, such as a driver's license. Finally, vendors require transaction authorization to determine if the purchaser actually has the funds to pay for the purchase.

Technological answers exist to provide these characteristics on-line. For example, digital signatures provide authentication over the Internet. Error checking algorithms and hash totals verify the integrity of messages throughout transmission. Finally, encryption contributes to secure communications between a purchaser and a vendor and prevents unauthorized parties from reading the information. Some general practices for encryption include SSL, PKI, RSA, and DES.

The availability of products and solutions to implement e-commerce is very fluid. With this fluid environment comes a fear of taking risks and making the wrong technological choice that will become obsolete. However, taking a "wait and see" attitude to avoid making the wrong choice also represents a risk. If the Commonwealth fails to make technological choices, even if they are the wrong choices, they will not successfully and completely implement e-commerce.

Twenty years ago, the home video industry faced a similar dilemma. Two video formats, Beta and VHS, were available to consumers and people were forced to make a choice by selecting one format. Those selecting the least popular Beta format soon found themselves owning an obsolete technology. Five years ago there were also struggles for some companies in selecting between two popular networking software products, Novell and NT. Businesses were concerned that they may choose the least popular product and encounter obsolescence; however, both products are still highly popular today.

To successfully implement e-commerce it is important for the Commonwealth to develop a set of standards; however, this involves much more than selecting technologies. It also involves establishing minimum requirements and guidelines. For example, when the Commonwealth decides on security over data transmissions, this should be communicated through guidelines that establish the minimum data transmission requirements. These guidelines would provide agency management, security officers and system administrators with guidance to follow when establishing their e-commerce systems, policies, and controls.

E-commerce guidelines must also provide specifications to the vendors and citizens wanting to conduct business with the Commonwealth. For example, the Commonwealth must establish and communicate the minimum information requirements and its format when accepting electronic invoices.

RECOMMENDATION #1

The Secretary of Technology must establish information technology guidelines and standards for agencies to follow when implementing e-commerce. He must communicate the minimum acceptable guidelines on which agencies can build their e-commerce systems. For example, if agencies must provide encryption for securing credit card payments by citizens, then this must be contained in the guidelines. Further, if the Secretary believes there must be encryption interoperability between agencies, then he should select a standard encryption technique.

E-Commerce Governance

The Virginia Public Procurement Act, Code of Virginia, Section 11-35 et seq, provides the basis for all public purchases by state agencies and institutions, as well as local governments. The Departments of General Services, Accounts, and Treasury set regulations for state agencies and institutions, including how the Commonwealth deals with vendors and others for the purchase and payment of goods and services.

However, no single department, agency, or institution has the statutory and regulatory oversight of the Commonwealth's revenue collections. The various entities that collect revenue have the responsibility for the billing, collection, and assessment processes, and their individual systems must support these functions.

Statutes set the amount and use of collections for the Commonwealth's taxes, licenses, and other revenues and allow for multiple payment methods. Currently, the Code of Virginia states that agencies accepting credit card payments may collect a credit card fee of four percent (4%) of the payment, in addition to the required payment. Only the Circuit Courts are required to collect this fee. Credit card fees are normally a negotiated and contracted percentage of the transaction. The percentage relates to the dollar amount and volume of transactions processed.

Questions arise as to who should pay the credit card fee, such as: If the entity does not collect both a tax and credit card fee has the taxpayer paid less than the full amount of the tax? Does not collecting the credit card fee penalize others that use either cash or checks? What is the base payment amount?

Each agency must establish individual policies over the collection of these credit card fees. Some agencies, such as the Department of Taxation, must collect the credit card fee because they do not have an appropriation to offset the cost. Other agencies, such as the Department of Motor Vehicles, save enough funds by having the taxpayer use the Internet and pay by credit card, that they absorb the cost of the credit card fee.

RECOMMENDATION #2

The General Assembly should re-evaluate the assessing of fees when citizens pay Commonwealth taxes, licenses, and other revenues by credit card. The General Assembly may wish to encourage the waiving of the credit card fee where agencies can demonstrate that the use of credit cards can reduce processing costs and losses due to bad checks or other receivable related costs.

In an electronic commerce environment, agencies may capture and store citizens' personal credit cards and agency small purchase charge card information as part of the e-commerce transaction record. We reviewed the Virginia Freedom of Act, Section 2.1-340 et seq., the Personal Information Privacy Act, Section 59.1-442 et seq., and the Privacy Protection Act, Section 2.1-377 et seq., which we believe exempt from disclosure personal credit card and agency small purchase charge card information. However, some agencies have questioned the need to specifically address an exemption for this information in the Freedom of Information Act.

RECOMMENDATION #3

The General Assembly may wish to determine if the Virginia Freedom of Information Act should provide additional protection of credit card information.

As stated above, the governing statutory authority for all purchasing of goods and services is the Virginia Public Procurement Act. We reviewed this Act and the related regulatory guidance given by the Departments of General Services and Accounts. Our observations concerning these matters are as follows.

Sections 11-35.G and 11-48 of the Code of Virginia state that "…all qualified vendors have access to public business and that no offeror be arbitrarily or capriciously excluded…" and further states that all public bodies shall "…facilitate the participation of small businesses and businesses owned by women and minorities in procurement transactions." While the Governor's Task Force on Procurement report stated that e-commerce would provide more opportunities for minority, women, and small businesses, we have found no studies that support or disprove this conclusion. In order to participate in e-commerce, these businesses may need to invest in hardware and software that will allow them to access and conduct e-commerce transactions such as bidding, billing, accepting payment, and exchanging inventory information. These businesses may find the hardware and software costs prohibitive.

To meet the Procurement Act mandates and maximize participation from targeted businesses, purchasing officers may need to continue manual processes. By continuing manual processes, they may not fully implement e-commerce and realize the expected cost savings. Sufficient information from other states or independent studies does not exist to estimate the cost of continuing current practices.

RECOMMENDATION #4

Since the Virginia Public Procurement Act, Sections 11-35.G and 11-48 of the Code of Virginia, provides policy statements concerning how the Commonwealth performs business, the General Assembly may wish to support DGS' e-procurement initiative and allow them to move forward, but require DGS to monitor and periodically report the status of including small, women, and minority owned businesses. Further, the General Assembly may wish to permit some pilot projects to operate using either e-commerce alone or a combination method. After some period of time, the pilot projects could report on their costs and whether they achieved the access envisioned by the Virginia Public Procurement Act. Based on these pilots, the General Assembly could determine the most appropriate action to take concerning these policies.

The Code of Virginia often states that transactions and documents must be "written" or "in writing" (Specific Code sections of the Virginia Public Procurement Act include §§11-37; 11-40.C; 11-41; 11-45.G, H and K; 11-46.1; 11-55.A; 11-62.11.1.B; 11-63; 11-66; 11-69; 11-71; and 11-79.1.). We believe the passage of the Uniform Electronic Transaction Act (UETA) addresses these issues and makes electronic records and signatures legally enforceable.

However, UETA does not resolve all issues arising from the implementation of electronic transactions. For example, the Code of Virginia, in a number of circumstances, requires a specific manner of delivery such as delivery by the U.S. Postal Service. UETA does not apply in such circumstances.

RECOMMENDATION #5

All agencies should review their applicable Code of Virginia sections in light of the exceptions outlined in the Uniform Electronic Transactions Act (UETA), Section 59.1-508(b) of the Code of Virginia, and recommend appropriate changes to accommodate e-commerce.

The Virginia Public Procurement Act also includes specific requirements concerning competitive sealed bidding and competitive negotiations, which fall outside of the provisions of UETA (See Sections 11-37, 11-41, 11-45.1, 11-46; 11-52.C and C.1, 11-54, 11-65, and 11-78.1). These requirements affect the operations of major purchasers such as the Department of Transportation and the move towards e-commerce bidding will significantly impact their procurement processes.

RECOMMENDATION #6

The General Assembly may wish to request that the Departments of General Services, Transportation, and Technology Planning study methods and technologies that the Commonwealth can use to implement electronic sealed bids and determine whether there are any modifications needed to existing code sections. The Departments should complete their work and report to the Joint Commission on Technology and Science by the start of the 2002 General Assembly session.

Much of the daily implementation guidance for procurement, payment, and revenue collection comes from the Departments of General Services and Accounts. Both Departments have issued manuals that define these requirements and processes.

The Code of Virginia, Section 2.1-442, gives General Services the authority to interpret the Procurement Act and establish rules and regulations. General Services communicates their rules and regulations through the Agency Procurement and Surplus Property, Capital Outlay, and Vendor Manuals.

The Agency Procurement and Surplus Property Manual establishes the policies and procedures for agency procurement within their delegated limits. The Capital Outlay Manual contains guidance, procedures, and policies that agencies must follow in the planning, design, and execution of all capital outlay projects. The Vendor Manual sets rules for the purchase of goods and non-professional services for vendors doing business with the Commonwealth.

The Code of Virginia, Section 2.1-196.1, requires the Comptroller to set accounting policies and procedures which he communicates through the Commonwealth Accounting Policies and Procedures Manual (CAPP Manual), maintained by Accounts. The CAPP Manual documents the policies and procedures associated with the Commonwealth's centralized accounting and financial systems. The Manual consists of 145 topics and spans over 2,400 pages.

Agencies view General Services and Accounts as leaders in setting and interpreting policy and rely on these manuals to govern how they operate. These manuals originated before the development of, and do not always accommodate, e-commerce. However, these manuals can accommodate e-commerce with some minor changes. Accounts has already begun functionally moving towards e-commerce by making vendor payments and transfers to localities using EDI.

RECOMMENDATION #7

The Departments of General Services and Accounts should update their manuals to allow for the use of e-commerce.

Centralized E-Procurement Solution

The Department of General Services has begun the process of implementing e-commerce by contracting for end-to-end procurement services known as the Commonwealth's E-procurement Solution (e-procurement). E-procurement will allow agencies and vendors, through a single Commonwealth portal on the Internet, to access an electronic mall (e-mall), a purchasing system, and other purchasing features.

A service contractor will provide its own hardware and software necessary to support e-procurement. Further, the contractor must have adequate back up and recovery plans and built-in redundancies for continuous access. The contract will contain appropriate separation clauses to protect the Commonwealth's data should the contract cease.

Agencies will access e-procurement through General Services' Capitol Campus Backbone, Department of Information Technology's COVANET, or Network Virginia. Those agencies without access to these services will connect through an Internet Service Provider.

General Services envisions e-procurement facilitating the purchasing of goods and services and leveraging of the Commonwealth's buying power. E-procurement will support those agencies with or without existing purchasing systems. General Services will provide central coordination while allowing agencies local control over the purchasing process.

E-procurement will provide for central vendor registration, e-mail to vendors with procurement opportunities, virtual surplus inventory, and a reverse auctioning tool. However, the main features will be the e-mall, purchasing system, and data warehouse.

The e-mall will identify state contracted goods and services and mandatory sources, as well as provide a dynamic catalog of items offered by registered vendors. Agencies can procure small dollar commodities and services through this location, which comprises the majority of purchases in the Commonwealth. This service will list vendors unable to conduct Internet business.

The purchasing system will provide a method to electronically requisition goods and services. Agencies will use the system to electronically create and post Invitations for Bids and Requests for Proposals, receive bids and proposals, and award the final contract. Currently, agencies must follow strict regulations for competitive sealed bidding

such as public posting, receipt, openings, and announcements. Sealed bidding generally involves high dollar long-term projects and General Services needs to build vendor trust in this new process.

Several concerns arise when considering the competitive sealed bidding process using this new system, including: data integrity, authentication, and non-repudiation. Data integrity controls verify that the bid received is complete, unaltered, and remains secure until public opening. Authentication controls validate the signer of a sealed bid. Non-repudiation controls prevent vendors from disclaiming the sealed bid. The Internet poses new threats and vulnerabilities to the procurement process and a lack of sufficient controls could lead to a compromised process.

Encryption, Public Key Infrastructure, and digital signatures tend to be the dominating technologies for ensuring data integrity, authentication, and non-repudiation. Not all documents involve sensitive or critical data; therefore, all documents do not need the same level of security.

RECOMMENDATION #8

Before implementing competitive sealed bidding through e-procurement, the Department of General Services must develop data integrity, authentication, and non-repudiation controls, manual or electronic.

General Services plans for the data warehouse to capture purchasing transactions and allow for standardized and ad hoc reporting to help leverage the agency and Commonwealth's buying power. However, the warehouse will automatically capture only purchases made through this e-procurement process. General Services recognizes that agencies will continue to purchase outside of the portal by phone solicitations, use of internal systems, and traditional competitive sealed bidding methods. To capture this information in the warehouse, agencies must extract information from their system into a standard format. Agencies will have to bear the cost of any customized interface development to facilitate this process.

RECOMMENDATION #9

The Secretaries of Administration and Technology should support the Department of General Services' initiatives by mandating the transfer of purchase data to the central data warehouse. With complete purchasing data, General Services would be able to analyze purchasing information and better leverage the Commonwealth's buying power. Further, they should encourage the use of the portal to facilitate a more efficient procurement process.

RECOMMENDATION #10

Agencies who do not use e-procurement should cooperate with the Department of General Services to transfer purchase information to the data warehouse. Complete statewide purchase information would facilitate General Services' review and analysis to identify statewide contracting opportunities.

General Services plans that e-procurement purchases will rely on the Small Purchase Charge Card (the purchasing card) program as well as electronic invoicing for payment.

The purchasing card eliminates individual vendor invoices by consolidating them into one monthly American Express invoice, reducing the volume of accounts payable transactions and administrative costs. We are concerned that the Commonwealth pays only for goods and services it has received. Charge card payment at the time of purchase over the Internet eliminates this basic control. Another concern with the expanded use of the charge card is the management of the Commonwealth's cash flow. The Departments of Accounts and Treasury have developed systems that allow the Commonwealth to pay its bills on time and maximize interest earnings on our funds. Expanding the use of the charge card program could make predicting cash flow needs much more difficult.

The small purchase charge card has eliminated much of the state accounting for petty cash purchases and reduced the amount of paperwork for purchases under $1,000, however the program does not provide certain control and accounting information. Agencies record the original monthly payment of the small purchase charge card in an account called "Charge Card Purchase of Supplies and Materials." Accounting departments must manually examine each purchase on a summary of activity, if the agency wants to allocate the cost in the account to various cost centers, programs, funds or other activities. Under e-procurement, General Services expects that agencies can use system features to reconcile the charge account and allocate the costs automatically, resulting in efficiency savings.

The Commonwealth has been making payments electronically since 1994 using electronic data interchange (EDI). With EDI transactions, the Commonwealth has the ability to assure the receipt of the goods and services; can adopt electronic purchasing, invoicing, and other payment methods to reduce accounting work; and finally, can continue to manage its cash flow and maximize interest income. Last year, the Commonwealth had partnership agreements with 3,245 vendors and made payments totaling approximately $12 billion.

RECOMMENDATION #11

The Department of General Services should encourage the use of electronic invoicing as a preferred payment option, particularly for contractors and suppliers of more costly goods and services. Further, they must carefully evaluate the risks associated with expanding the use of the purchase charge card.

General Services envisions a phased in implementation for e-procurement with the e-mall, vendor data warehouse, purchase data warehouse, and electronic posting components

occurring on March 1, 2001. The remaining portions of e-procurement will be operational by year-end 2001. However, General Services views these services as dynamic and there will be additional modifications over time.

Auditability

The success of e-commerce relies not only on addressing statutory and regulatory barriers and obstacles, but also on determining that the process has adequate controls and audit trails to analyze and review transactions. In determining auditability, we considered the needs of our Office and other auditors, as well as the daily needs of accounting managers and staff to review and analyze their work, and the agency's management to receive reliable and accurate information.

This Office has a responsibility for auditing all public accounts and consistently encounters agencies that use automated accounting and information systems. E-procurement is simply another form of an automated accounting and information system.

Automated controls are the same as those expected for traditional manual controls; however, achieving these controls occurs differently. For example, separation of duties occurs in an automated environment by controlling access to critical functions through user ids and passwords. Also, audit trails no longer exist as hardcopy forms with physical signatures, but instead exist as electronically stored purchasing records authorized by electronic signatures.

Much of the work and information that accounting and fiscal managers use on a daily basis are the essential controls that make the system reliable and auditable. These controls, such as the reconciliation of bank accounts and daily cash settlements, provide external verification of the completeness and accuracy of the automated system. Electronic systems need controls not only for the external auditor, such as our Office, but also so that management receives accurate and reliable information about the agency's operations.

The Department of Technology Planning, formerly the Council on Information Management, has issued a number of comprehensive standards that address sound approaches to the development, documentation, and implementation of internal controls for electronic systems. All agencies and institutions must comply with these controls and they serve as the basis for what we believe are the fundamental controls for auditability.

Government Auditing Standards, issued by the United States General Accounting Office, defines the standards that government auditors must follow when planning, executing, and reporting a financial audit. In order to perform our audits in accordance with these standards we must gain an understanding of internal controls, assess risk, and design appropriate audit procedures to meet the audit objectives. Additionally, these standards require that auditors document their understanding of the computerized systems used during an audit.

We have long recognized the technology initiatives of the Commonwealth and we expect all staff to understand system controls and to design and execute appropriate audit procedures. To facilitate this expectation, we have set a goal of having all staff with base competencies in accounting information systems and computer security. Therefore, we

provide on-the-job as well as formal training to all our staff, and some have earned the Certified Information Systems Auditor designation. We also recruit new staff having education and experience in accounting and computer related technologies.

For audit procedures requiring more technical knowledge, we have audit specialists with advanced audit skills in specific disciplines, such as information security and telecommunications. These audit specialists have acquired the technical training and experience that allows them to evaluate and test system controls. For agencies using e-commerce, we would expect that our audit would review the controls for the following items:

- A documented information security program and documentation that includes a risk assessment, business impact analysis, and contingency, backup, and disaster recovery plans.
- The assignment of the information security responsibility to one individual. This individual should oversee security awareness training within the agency to help employees understand their security responsibilities based on their job responsibilities.
- Access controls, which restrict access to resources and allow access only to privileged entities. These controls should include policies for granting different levels of access to information.
- Termination procedures for ending an employee's employment or external users access.
- Physical access controls, which limit access to an agency's hardware and software.
- Authentication controls that ensure only properly authorized individuals use agency information, prevent data alteration or destruction in an unauthorized manner, and provide a mechanism to verify an entity or individual.
- Transaction trails that follow transactions through the accounting system and approval process and provide for electronic retrieval of transactions at a later time.
- Record retention policies and practices that identify the records and transactions necessary for retention.
- Audit controls, which allow the agency to identify suspect data access activities, assess its security program, and respond to weaknesses.
- Systems development and maintenance controls that provide for the proper testing and authorization of application updates and modifications.
- System configuration controls, which provide guidance over the installation and administration of hardware and software.

Agency management has responsibility for developing and maintaining a system of internal controls, which ensures that records are accurate, authorized, and complete. Management must document these internal controls in policies and procedures and effectively communicate them to employees. Transitioning to e-commerce will require agencies to re-examine their business rules and re-determine where they need to improve or enhance critical internal controls. Agency internal auditors can help managers verify that their departments are complying with the system of internal controls with reviews that focus on economies and efficiencies of specific procedures.

RECOMMENDATION #12

Given the dynamic environment, agencies should recognize the need for continuous training of managers and internal auditors on electronic commerce and the changes in business processes and internal controls that can result. The Department of the State Internal Auditor may be a resource to provide necessary training.

Conclusion

Our study identified some statutory and regulatory barriers or obstacles, which may impede the implementation of electronic contracting and procurement processes. The resolution of these obstacles and barriers are critical to the successful implementation of e-commerce in the Commonwealth. Further, we have determined that audits of public accounts can satisfactorily occur in an e-commerce environment.

RECOMMENDATION #1

The Secretary of Technology must establish information technology guidelines and standards for agencies to follow when implementing e-commerce. He must communicate the minimum acceptable guidelines on which agencies can build their e-commerce systems. For example, if agencies must provide encryption for securing credit card payments by citizens, then this must be contained in the guidelines. Further, if the Secretary believes there must be encryption interoperability between agencies, then he should select a standard encryption technique.

RECOMMENDATION #2

The General Assembly should re-evaluate the assessing of fees when citizens pay Commonwealth taxes, licenses, and other revenues by credit card. The General Assembly may wish to encourage the waiving of the credit card fee where agencies can demonstrate that the use of credit cards can reduce processing costs and losses due to bad checks or other receivable related costs.

RECOMMENDATION #3

The General Assembly may wish to determine if the Virginia Freedom of Information Act should provide additional protection of credit card information.

RECOMMENDATION #4

Since the Virginia Public Procurement Act, Sections 11-35.G and 11-48 of the Code of Virginia, provides policy statements concerning how the Commonwealth performs business, the General Assembly may wish to support DGS' e-procurement initiative and allow them to move forward, but require DGS to monitor and periodically report the status of including small, women, and minority owned businesses. Further, the General Assembly may wish to permit some pilot projects to operate using either e-commerce alone or a combination method. After some period of time, the pilot projects could report on their costs and whether they achieved the access envisioned by the Virginia Public Procurement Act. Based on these pilots, the General Assembly could determine the most appropriate action to take concerning these policies.

RECOMMENDATION #5

All agencies should review their applicable Code of Virginia sections in light of the exceptions outlined in the Uniform Electronic Transactions Act (UETA), Section 59.1-508(b) of the Code of Virginia, and recommend appropriate changes to accommodate e-commerce.

RECOMMENDATION #6

The General Assembly may wish to request that the Departments of General Services, Transportation, and Technology Planning study methods and technologies that the Commonwealth can use to implement electronic sealed bids and determine whether there are any necessary modifications to existing code sections. The Departments should complete their work and report to the Joint Commission on Technology and Science by the start of 2002 General Assembly session.

RECOMMENDATION #7

The Departments of General Services and Accounts should update their manuals to allow for the use of e-commerce.

RECOMMENDATION #8

Before implementing competitive sealed bidding through e-procurement, the Department of General Services must develop data integrity, authentication, and non-repudiation controls, manual or electronic.

RECOMMENDATION #9

The Secretaries of Administration and Technology should support the Department of General Services' initiatives by mandating the transfer of purchase data to the central data warehouse. With complete purchasing data, General Services would be able to analyze purchasing information and better leverage the Commonwealth's buying power. Further, they should encourage the use of the portal to facilitate a more efficient procurement process.

RECOMMENDATION #10

Agencies who do not use e-procurement should cooperate with the Department of General Services to transfer purchase information to the data warehouse. Complete statewide purchase information would facilitate General Services' review and analysis to identify statewide contracting opportunities.

RECOMMENDATION #11

The Department of General Services should encourage the use of electronic invoicing (EDI) as a preferred payment option, particularly for contractors and suppliers of more costly goods and services. Further, they must carefully evaluate the risks associated with expanding the use of the purchase charge card.

RECOMMENDATION #12

Given the dynamic environment, agencies should recognize the need for continuous training of managers and internal auditors on electronic commerce and the changes in business processes and internal controls that can result. The Department of the State Internal Auditor may be a resource to provide necessary training.

The General Assembly created the Joint Commission on Technology and Science (JCOTS) in 1997 as a permanent legislative commission with the goal of studying technology and promoting the development of technology and science. JCOTS generally conducts studies using advisory committees. Currently, there are six advisory committees.

In November of 1999, the e-government advisory committee met to learn about the current state of electronic government and to make suggestions about ways JCOTS could continue to support electronic government efforts. Some of the suggestions included:

- Supporting the Department of General Services' electronic procurement plan;
- Identifying and eliminating barriers to electronic contracting and procurement that may exist in Virginia Code or agency regulations;
- Amending Virginia's current statute on electronic signatures; and
- Determining whether the statutory and regulatory requirements of the State Internal Auditor and the Auditor of Public Accounts would be satisfied.

After review, JCOTS initiated Senate Joint Resolution 72 (SJR 72), which required the Auditor of Public Accounts to study statutory, regulatory, and auditability obstacles and barriers to electronic procurement.

Before the SJR 72 study, the 1998 General Assembly directed the Department of Technology Planning to perform a study, Senate Joint Resolution 36 (SJR 36), to determine methods of electronic contracting and procurement under the Procurement Act. The study determined that the goals of implementing electronic contracting and procurement were to reduce paper, increase productivity, provide more services at a lower cost, and make better use of technology. The study discussed the benefits as well as the impediments to electronic contracting and procurement.

Benefits included increasing buyer productivity, expanding the supplier base, better managing information, as well as allowing a wider availability of catalogs and contracts. The primary impediments focused on legal restrictions such as the use of the word "written" within the Code of Virginia. The study also recognized there were practical impediments such as standardization, infrastructure, security, and vendor buy-in.

Also in 1998, Governor Gilmore announced the creation of the Council on Technology Services (COTS), whose objective is to develop the framework to handle state government information technology planning and decision-making. Simultaneously, the Governor appointed the first Secretary of Technology, who serves as the Chairman of COTS.

During 1999, the Governor issued Executive Order 51, which established a direction for the Commonwealth's virtual government. This order set policies for executive branch agencies to develop plans for delivering current and expanded services through the Internet. It also orders that agencies make available all forms citizens need via the

Internet by December 31, 2000. Finally, agencies must follow the Secretary of Technology's guidance regarding digital signatures.

In late 1999, COTS established the Digital Signature Initiative (DSI) Work Group to help determine the Commonwealth's policies over this technology and any audit issues. There are 12 pilot teams conducting a series of parallel demonstrations using public key infrastructure and digital signatures. The DSI concluded in September 2000 with a report on their findings and recommendations. Their report recommended that the Commonwealth deploy digital signature and PKI technology strategically and that an enterprise solution of trust should be adopted.

In 2000, Governor Gilmore issued Executive Order 65 to accelerate and implement e-government and related technology initiatives. These initiatives include the creation of the Electronic Government Implementation Division, the implementation of e-procurement, the development of other web based administrative tools, and the encouragement of sound security and privacy policies.

Recent Legislation

Federal and state governments have passed legislation within the past year for conducting business electronically. The Commonwealth enacted the Uniform Computer Information Transactions Act (UCITA) and the Uniform Electronic Transactions Act (UETA). In June, the President signed the Electronic Signatures in Global and National Commerce Act (E-Sign Law).

UCITA provides uniform rules governing contractual transactions for intangible goods, such as computer software, Internet and online information, licensing agreements, and computer databases. The provisions of this act will become effective on July 1, 2001.

UETA provides rules and procedures for using electronic records and electronic signatures in both commercial and governmental transactions. UETA prevents electronic transactions from being invalid simply because they are electronic.

The new E-Sign Law will supersede both preexisting and future state laws, with the exception of those states, such as Virginia, that are in compliance with the UETA.

DES - Data Encryption Standard

A symmetric method of encryption that uses the same key to encrypt and decrypt.

EDI - Electronic Data Interchange

A national standard format used to exchange business data between two or more business partners electronically. The American National Standards Institute administers this standard.

Encryption

Putting data into a secret code so it is unreadable except by authorized users.

EFT - Electronic Funds Transfer

The transfer of funds by means other than paper instruments.

FTP - File Transfer Protocol

This protocol allows for the efficient transfer of whole files from one computer to another via the Internet.

HTTP - Hyper Text Transfer Protocol

The protocol used to transfer data over the World Wide Web.

HTML - Hyper Text Markup Language

This language is used to create web pages. For a web page to appear correctly in a web browser, this standard language must be used. Most web pages are written with another generator that creates the HTML.

PKI - Public Key Infrastructure

This is an asymmetric method of encryption using two mathematically related but different keys. If a public key is used to encrypt, then only the corresponding private key can decrypt and vice versa.

RSA - Rivest, Shamir, and Adelman

A public key algorithm used to encrypt data (see PKI). This algorithm is named after its creators.

SSL - Secure Sockets Layer

This protocol is from Netscape Communications Corporation and allows for a secure method of communicating over the Internet.

TCP/IP - Transmission Control Protocol/ Internet Protocol

This protocol allows communications via the Internet. The IP portion allows data to be sent in small packets between nodes. Each packet may get to its destination via a different path. The TCP portion verifies delivery of packets.