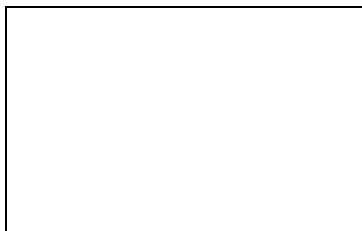


The Enterprise Portal:
Organizational Issues
Funding and Related Concerns
Data-Sharing

A White Paper
NECCC
December, 2000



National Electronic Commerce Coordinating Council

The National Electronic Commerce Coordinating Council (NECCC) is an alliance of national state government associations dedicated to the advancement of electronic government within the states. The Council is comprised of **NASIRE** (a group representing the chief information officers of the states), the National Association of State Purchasing Officials (**NASPO**), the National Association of State Auditors, Comptrollers and Treasurers (**NASACT**) 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 (**NACHA**). The ITAA and the NACHA specifically represent private information technology companies and the financial services and technology industries.

EXECUTIVE BOARD

Chair: **Hon. J.D. Williams**, NASACT, Idaho State Controller

Vice Chair: **Richard B. Thompson**, NASPO, Maine Director of State Purchasing

Secretary/Treasurer: **Carolyn Purcell**, NASIRE, Executive Director, Texas Department of Information Resources

NECCC BOARD

NASIRE	George Boersma , CIO & Deputy Director, Michigan Department of Management & Budget Steve Kolodney , Director, Washington Department of Information Services
NASPO	Dave Ancell , Director, Office of Purchasing, Michigan Department of Management & Budget Joyce Murphy , Director, Division of Purchasing & Materials Management, Missouri Department of Administration,
NASS	Hon. J. Kenneth Blackwell , Ohio Secretary of State, Hon. Elaine Marshall , North Carolina Secretary of State Hon. Ron Thornburgh , Kansas Secretary of State
NASACT	Hon. David Heineman , Nebraska State Treasurer Hon. Thomas Wagner , Delaware Auditor of Accounts
NGA:	Thom Rubel , National Governors Association
NASCA	Pam Ahrens , Director, Idaho Department of Administration
ITAA	Basil Nikas , CEO, iNetPurchasing.Com
NACHA	William Kilmartin , Vice President, American Management Systems - AMS

NECCC STAFF

Brandon W. Lenoir, Director • 202-624-5451 • e-mail: blenoir@nasact.org • web: www.ec3.org

ACKNOWLEDGEMENTS

This White Paper was prepared by the NECCC Integrated Services and Portals Workgroup.

CONTRIBUTORS:

Tom Little	General Manager	Business Development, SCT.
Odysseus Marcolpus	Director, Office of e-Government	New Jersey Office of Information Technology;
Georgia Marsh	Associate Director	Illinois Department of Revenue;
Mark Struckman	Director of Research Programs	Center for Digital Government;
Pam Sutton	e-government Program Manager	Nevada Department of Information Technology;

Mr. Little also served as editor; Mike Teller, of Lockheed Martin, served as the group's original chairperson; and Brandon Lenoir, of the NECCC staff, provided outstanding administrative and coordinating support.

Table of Contents

PAGE

4. INTRODUCTION

5. ORGANIZATIONAL ISSUES

Washington

North Carolina

Illinois

PKI

GIS

To-Do List

The New Infrastructure of Digital Government

Resources

11. FUNDING

Government-Developed and Funded

Commercially-Developed and Government-Funded

Commercially-Developed and User-Funded

Commercially-Developed and Funded through Combinations

To Charge or Not To Charge

Funding and Privacy

Funding in the Future

18. DATA-SHARING

The Promise

The Reality

Business Objectives

Functional Requirements

System Design

Other Phases of the Software Development Lifecycle

26. CLOSING THOUGHTS

Introduction

Electronic government and electronic commerce are rapidly and dramatically changing the way the public sector interacts with its constituents. Public expectations, coupled with the possibilities created by new technologies, make this Internet-based evolution (or is it “revolution”?) a top priority within many governments.

Governments are rapidly moving from web sites with static presentations of information to function-rich sites that afford citizens the opportunity to interact with their governments in many ways. However, because there is little experience to draw upon, there are no clear “best practices” to follow and the path to true electronic government is beset by hazards and challenges of many types.

This white paper is divided into three sections – Organizational Issues; Funding; Data Sharing – and is intended to provide some insight into several key issues involved in creating an enterprise portal for a city, county, state or agency. It is not intended to be all-encompassing and, by the very nature of this dynamic environment, some of the data will be aging even as this paper is being published.

While this paper does not purport to answer every question, it does identify significant issues that should be addressed in establishing plans and policies related to a portal. As IT managers and government executives approach portal development projects, they should do so fully expecting that the path may not always be smooth and that organizational, financial, policy and technology challenges may be frequent.

Organizational Issues

After much experimentation, most government IT officials now support the concept of developing an enterprise portal that gives a jurisdiction's web site a consistent quality and facilitates easy navigation for citizens. The information that follows focuses on three states that have become recognized leaders early in the e-government arena and that were early adopters of the enterprise-wide concept: Washington, North Carolina and Illinois.

This paper considers critical elements in enterprise portal planning and includes an analysis of a new infrastructure for digital government, based on observations from the Center for Digital Government. The framework presented here will likely support the varied requirements of individual states.

WASHINGTON

The state of Washington intends to make all relevant information and services available to businesses and citizens through its portal within the context of established guidelines. The policies developed by state IT officials apply specifically to "external content" and not to the intranets accessible only to employees. Intranet use, e-mail and other internal applications are governed by policies restricting their use to official state business.

Washington agencies may include information on their web site from entities that are not part of state government. The policies make clear, however, that the state's web site is not a "public forum" and that agency decision-makers may use their discretion about including information from other sources. Agencies do not have the option of eliminating content required by law or that constitutes official government business.

The policy also states that certain information from other sources may be beneficial to the state's web site and to the public. These external sources may include links, acknowledgments and advertisements, along with other items, as there are many resources outside of agency control offering information and services that may benefit the public. In addition, public acknowledgment of sponsors and contributors may help the agency to expand its online resources while advertising revenues could potentially defray the cost of operating the government web site.

The policy specifically describes content that is not acceptable. This includes, but is not limited to, political advocacy, the promotion of specific people, content not suitable for minors, the promotion of drugs or weapons, subjective statements about various products or services, trademark infringements and content that does not support the integrity of the agency. These exceptions also apply to links from the web site. Using best judgment and discretion, agencies have the right to exclude external content that does not meet the stated policy guidelines.

According to CIO Steve Kolodney, there is an ongoing effort to educate legislators about IT issues and what is required to implement e-government. The fact that Washington has won a number of accolades and awards for its IT achievements has assisted in communicating the importance of the e-government mission to legislators and

the governor. In addition, since interagency collaboration is a critical part of the state's plan, constitutional officers have become key partners. The state seeks the "buy-in" of department heads and constitutional officers, knowing their leadership is crucial to the success of the overall plan.

NORTH CAROLINA

North Carolina has also been at the forefront of the digital revolution. Governor Jim Hunt and the legislature have actively supported the Department of Information Technology Services (DITS), easing the state's transition to e-government services. A major facilitator was SB 222, a bill that covered a wide range of IT issues and has become a model for other states' IT legislation.

The bill stipulated that North Carolina would have one portal and all the state's agencies would be accessed through that single point of entry. According to DITS officials, agencies have willingly participated in development of the portal. Each agency is responsible for its own content and for links included on the agency page. To track changes, the state has a process in which agencies notify DITS and, conversely, DITS officials alert agency heads to alterations and additions they have made to the portal. The spirit of respect and cooperation is further observed in the policy of DITS managers asking permission of agency public information officers (who are responsible for agency sites) to use specific items appearing on the agency's pages.

DITS officials have adopted the attitude that agencies know best what their customers want. The department's role is to get the information out in a consistent, format. The portal and its wealth of information have become so popular that an increasing number of outside organizations are asking for links on agency sites. Consequently, the state is developing a set of policies to guide agency decisions related to outside links.

North Carolina includes privacy statements on agency pages and its home page.

Department officials say one of the biggest challenges has been integrating local governments into the portal. The many different levels of sophistication among the state's municipalities have made this integration process slower than anticipated.

North Carolina has developed a number of common services in critical areas such as credit card acceptance. Although agencies are not required to use the central system, IT officials report across-the-board participation. The state was able to negotiate very favorable rates with the central credit card acceptance program, and receives economies-of-scale savings that would be unavailable to an individual agency. In addition, DITS is setting up a PKI infrastructure to enable agencies to authenticate users and implement digital signatures.

The state is also building an e-forms service. This central repository of forms will store data on individual transactions with various state agencies, thus eliminating the need for citizens or businesses to submit the same information countless times. To engage the agencies, DITS is considering a program in which it would offer to develop the top five

forms for each agency, at no charge. Officials are confident this service will create a high level of participation throughout the agency system.

North Carolina's web site is based on a number of common principles, although each agency retains its independence; agency autonomy is balanced with the enterprise view. With the goal of providing the best possible experience for citizens, developers are directed to follow a set of standard web design guidelines intended to offer the following functions: accessibility that addresses the needs of disabled citizens and others; design considerations that are user-friendly; a task-driven approach to navigation; use of informative hyperlinks; use of meta-tags to assist with search capability and documentation; web design that supports multiple browsers; web-based presentations that use HTML 4.0; and a test user environment that suits the needs of each agency's audience.

The state also recommends that agencies consider minimum hardware and software requirements that users will need to download documents and information.

ILLINOIS

Under the leadership of Governor George H. Ryan, Illinois has moved from a ranking of 49th in 1998 to 4th in the nation in 2000 for its use of digital technology, according to the Digital State Survey conducted by the Progress and Freedom Foundation and the Center for Digital Government.

Part of the state's significant investment in technology focuses on e-government. Among other things, the state is implementing an Information Technology Enterprise Planning System to promote common business models and shared technological infrastructure. The system will include criteria against which IT initiatives can be evaluated for funding, with heavy emphasis on enterprise-wide activities as well as those dealing with GIS, e-government, e-commerce, ERP, data warehousing and office application standards.

Using a task-driven, citizen-oriented model, Illinois has built a strong foundation on which to develop and operate enterprise-wide solutions. This foundation is composed, in part, of:

Public Key Infrastructure (PKI), which gives the state the capability to process highly sensitive information on systems and the ability to digitally sign electronic documents.

Geographic Information Systems (GIS), which can link data that are related by a geographic location, such as a county boundary, street address or Zip code. Since the data are related by location, they can be combined to solve a problem. Data can be associated with or related to three kinds of features: point, line and polygon.

PKI

The state's PKI provides an enterprise-wide infrastructure to facilitate electronic government services. It uses public key cryptography and digital certificates, along with the software to manage those certificates. Building this service into software applications

provides the means to authenticate users, ensure privacy and integrity of data, and establish audit trails needed to give electronic transactions the same or better levels of assurance than are afforded to paper transactions.

PKI provides a very workable model for citizens, eliminating the need to deal with multiple PINs, passwords, or encryption keys. PKI facilitates the use of digital keys by managing the life span of the keys, providing a mechanism to distribute, verify and revoke the keys and delivering software services that other applications can utilize to perform these functions. By integrating connections to these services in applications, the entire process is essentially transparent to the end user. The state's central management agency will serve as its certification authority and issue certificates. This certificate will enable the citizen to receive personalized electronic services, digitally sign documents for submission to any state agency, and send or receive sensitive information in an encrypted form, to protect privacy while interacting with the participating state government agency.

GIS

When presented on the web, GIS enables users to see statistical data overlays interactively, on a map of Illinois. Managing information from various agencies on visual layers helps government focus on issues, trends and opportunities relative to a geographic area. It assists citizens by providing a more comprehensive picture of Illinois' infrastructure in areas such as education, manufacturing, transportation, tourism, environment, taxation and site and building availability.

The state views GIS as a critical tool for promoting economic development and enabling Illinois to prosper in the global marketplace. This is especially true in the area of business planning, where the goal is to have the portal provide entities anywhere in the world 24/7 access to a full range of Illinois-specific information to help with their decision to start a business in the state and where best to locate. For example, an international corporation contemplating opening an office in Illinois will be able to access www.business.state.il.us, and click on the "New Business Planning" option. In a single visit, the corporation will be able to navigate to any city or county in the state and find vital data on building and site availability, tax base structures and workforce opportunities, as well as quality of life and education information.

To-Do List

The state has developed a "to do" list for portal development. While focused on state government, it could easily be transferred to cities or counties. The list includes:

1. Building a common framework that allows data transfer among agencies and with the public.
2. Establishing a single doorway through which citizens can fully access all levels of government.
3. Implementing projects that have a high value and can be quickly accomplished (e.g., within two years).
4. Providing the highest level of security, protecting data and transactions to the greatest possible degree.

5. Collaborating across organizational and jurisdictional boundaries to facilitate greater citizen accessibility and ease of use.
6. Enabling businesses to conduct all business with the state online.
7. Taking full advantage of economies of scale through statewide practices and procurements.
8. Removing policy and statutory barriers to full e-government (i.e. availability of e-notaries, return receipts).
9. Providing full, online access to the legislative process (i.e. e-mail, review of summaries and bills, web casting proceedings).
10. Involving state leaders in discussions that increase their awareness of technology opportunities and impacts on the future of the state.

Illinois has also developed a list of 10 keys to success for enterprise portals:

1. Easy to use
2. Universal Information Access
3. Dynamic Resource Access
4. Extensible
5. Collaborative
6. Customizable
7. Proactive
8. Secure
9. Scalable
10. Manageable

THE NEW INFRASTRUCTURE OF DIGITAL GOVERNMENT

Looking beyond specific states, the Center for Digital Government has reviewed a variety of plans for e-government infrastructure focusing on state government, and has done comparative analysis of actual implementation experiences. In this consideration, infrastructure is more than desktop devices, networks and mainframes or servers. It is a set of common services that can, and should, be maintained by a central organization within the jurisdiction.

The centralized infrastructure, by definition, crosses agency boundaries reaching across the enterprise with common tools and services. Because government has traditionally been a vertical structure composed of discrete agencies IT efforts have often been duplicated throughout organizations, consuming time and funds, and unintentionally creating incompatible systems. IT helps agencies to coordinate and collaborate on information and programs, but does not strip an agency of its individuality or mission.

Common digital government services include the following enterprise-wide elements:

- Payment acceptance services
 - Credit card processing
 - Electronic funds transfer

- Internet bill presentation and payment
- An enterprise portal
- Privacy and security
 - Access control
 - Identification/authentication
 - Data confidentiality
 - Data integrity
 - Non-repudiation
- A certificate authority & digital certificates
- E-forms/workflow processes
- Enterprise data warehouse
- Enterprise infrastructure help desk

RESOURCES

Washington has developed a Digital Government Academy to assist agencies in the transformation to e-government. The academy also helps agencies develop a common look and feel for the state's web site while maintaining variations that characterize each agency. Instruction includes technical skills as well as project management skills. Using the common elements in the state's Digital Government plan, agency participants are instructed in how to set up a site that is compatible with specific requirements, yet uniquely suited to their needs. The goal is to have participants return to their agencies equipped with the skills and knowledge to bring their agency online, develop and maintain content and effectively manage the process throughout the transition to e-government.

To support the integrity of IT projects, North Carolina developed a Management Certification Process. All projects costing more than \$500,000 or which are strategic in nature must go through this process. If an agency is not able to manage the certification process as outlined, the agency can contract with the centralized IT organization or an outside vendor for project management services.

These "digital states" show there is room for variation in the development of an enterprise portal. However certain elements are fundamental and shared. Most importantly, there must be consensus among the various agencies and organizations that the enterprise-wide approach is the most powerful and effective way to deliver digital services. Direction for acceptance of this concept begins at the top of state government and is implemented by CIO's, or other executives, who have been vested with appropriate authority.

Funding

While there is no generally accepted definition of what a government portal is, there is even less agreement about the “best” or “most appropriate” way to fund it, both in the short and long term. To date, several different models of portal development and funding have emerged. However, there are differing views of how these approaches will survive over the long term.

GOVERNMENT-DEVELOPED AND FUNDED

In a few cases where governments have been fortunate enough to have sufficient information technology skills and budgets available, in-house development of portals has been undertaken. Although in the minority, this approach gives the government total control over transaction fees or advertising. If fees are assessed, they remain with the government.

Iowa initially pursued a fee-for-service approach but subsequently abandoned that in favor of a self-funded model. The state has a \$12 million budget allocated for portal development and implementation in 2001.

North Dakota brought its initial portal online with an investment of \$15,000, using existing state IT staff, after deciding that they would not charge convenience fees. The state plans to add electronic commerce transactions incrementally.

The state of Washington, generally recognized as one of the most digitally-focused and advanced state governments, has developed and funded its portal operations internally, using general fund appropriations.

In addition to general fund appropriations, a few governments have issued bonds to fund portal initiatives and others have established special funds. Maryland, for example, established the Information Technology Investment Fund that includes an annual appropriation of \$1.5 million, plus certain commissions and right-of-way access charges.

COMMERCIALY-DEVELOPED AND GOVERNMENT-FUNDED

In this model, which retains a rather traditional relationship between government and technology vendor, governments contract with a commercial vendor to implement a portal, either as a custom development project or using an off-the-shelf product as the basis for the portal. The government retains complete control over the portal, as well as the convenience fees, if any, and retains sole rights to the data collected.

Some private consulting firms prefer to work with this model. North Carolina contracted with a private firm for a multi-phased portal development project, with more than \$3 million budgeted for the initial phase, including management of the state’s e-commerce initiatives.

COMMERCIALY-DEVELOPED AND USER-FUNDED

In the early stages of portal development and implementation, the trend in systems with financial transactions has clearly been toward systems developed commercially and funded through a transaction-based fee, often termed a “convenience” fee. In most cases, the government has been offered these systems with little or no investment and the vendor has gained the right to impose a fee to citizens using the systems. It is important to note that this convenience fee is in addition to the transaction fee tied to the processing of credit card payments – which are typically in the range of 2 percent of the transaction amount.

In the newly-emerging world of electronic government, where there is no history and only conjecture about how it will be received and used by the public, many governments are turning to the private sector to take on the risk. Colorado’s Chief Information Officer, Paul Quade, put it succinctly earlier this year when he said he wants vendors to make the total initial investment, “Basically, they would be taking all the risk.”

So far, there have been plenty of firms, typically funded with venture capital, willing to take that risk. In some cases, government and vendor share development costs and may share in the revenue generated from convenience fees or advertising on the portal. They may also share in revenue gained from the vendor’s sales of data collected or accessible via the portal.

Many private companies have been working diligently to establish a presence in the market with this model or a variation of it. However, several of these firms have also begun offering variations, which may include some licensing fees or advertising.

In most cases the company’s revenue is generated from user fees, and advertising and they share some revenue with their clients. Fees typically range from \$1 to \$5 per transaction. Several state governments have turned to the private sector for their initial portal development, as has the city of San Francisco, which is implementing a portal at no cost to the government. The company will charge a convenience fee related to the payment of traffic and parking fees, property taxes, online permitting, license renewal, some utility payments and other similar services.

As an adjunct to this user-funded approach, several states, including Indiana, charge firms for access to specific records. For example, they charge a fee to insurance companies for online access to driving records. This is a service every state already provides in some way – usually with staff tracking down files and providing paper copies for a fee.

The National Association of State Information Resource Executives (NASIRE) published a study in early 2000 – ***“Preliminary Survey of the Digital Government Landscape”*** – which showed that 11 of the 16 states that responded to the survey and indicated they are planning to build or expand a portal, planned to compensate the vendor through a transaction fee arrangement.

COMMERCIALLY-DEVELOPED AND FUNDED THROUGH COMBINATIONS

The inability of transaction fees to adequately fund projects has led to the creation of other models, including advertising. In some cases, projects may be funded by a combination of government appropriations, transaction fees and advertising. Several firms have developed in the past year with the primary purpose of managing the advertising process.

Advertising, raises a wide range of issues about the type of advertising that is acceptable, who “approves” advertising and who monitors links that might be created. Government positions on the topic range from welcome acceptance of advertising to complete rejection.

TO CHARGE, OR NOT TO CHARGE

When financial transactions occur on the web, there are virtually always added costs involved. In a few cases, governments have elected to accept only electronic checks, negating the costs associated with credit cards. *(For a more in-depth discussion about EFT, see the NECCC’s “Electronic Payments Primer” available in PDF at www.ec3.org.)*

In most cases, constituents will demand the ability to pay fees by credit card – just as they do on commercial sites. In virtually all of those cases, there is a transaction fee tied to the transaction. In a few cases, governments have been able to have the fee waived in return for allowing the supporting financial institution the benefit gained from maintaining a significant minimum deposit with the credit card network’s related bank.

In most cases it can be assumed government transactions on the web will be handled with a credit card. Most credit card companies prohibit any business from directly passing along that charge to consumers. However, the industry has approved the imposition of convenience fees. When implemented, those convenience fees will normally need to be sufficient to cover the transaction fee, plus any other expense the government expects to pay – such as maintenance of the portal. Some states are changing their laws to accommodate this new business model. In California, for example, a new law authorizes courts to collect fees equal to the “actual cost” of the transaction.

In those instances where a commercial vendor is allowed to collect the convenience fee, the amount must cover the transaction fee, plus an amount sufficient to enable the vendor to realize a profit, so commercial vendors must be able to project a sizable number of transactions in order to justify the expense they incur in developing and maintaining the portal.

Some governments are electing to absorb the cost associated with credit card transactions, following the premise that electronic processing is more efficient than manual processing, so the government’s operational costs are lower. Florida, for example, is absorbing credit card fees for a variety of transactions, such as a test real estate license renewal project, and for some online retail purchases.

One counter argument to the convenience fees question is: If conducting business electronically really does lower the government's operational costs, shouldn't the government actually discount fees paid via the web? Instead, citizens seeking services via the traditional, more costly in-person channels should pay a surcharge. This is similar to the banking industry, where a number of major banks are now charging their customers to interact with a teller, rather than using an ATM or online service.

The question of online vs. in-person costs won't be easily answered, because there are many variables. The fact that the web transaction reduces effort for the citizen doesn't necessarily translate to reduced work for the government staff. If the portal isn't tightly integrated with applications, thus automating processes inside the agency, the workload could even be greater. Value, in terms of reduced work, will come only when those processes previously handled manually are transferred to automatic electronic processes.

FUNDING AND PRIVACY

Governments have been collecting (and selling) data about individuals for many years. However, because this process of selling data has been both legal and largely unnoticed, there have been few complaints.

Now, as more and more data about individuals becomes accessible online, concerns about privacy are beginning to escalate. NECCC has recognized this and is publishing a white paper entitled, ***"Privacy Policies – Are You Prepared?"*** to address many of the issues related to the posting of privacy policies and concerns of the public.

There is a substantial market for data collected by governments. Imagine, for example, how valuable it is for credit organizations to have information about bankruptcy filings, or liens against individuals or companies, or data about substantial legal judgments against individuals or companies. Consider the value to a home security firm to have a list of all property transactions above a specific dollar amount, providing them with a source of potential clients. Perhaps a new auto maintenance firm wants to establish a client base. How valuable would a list of recent auto registrations be? It is not difficult to extrapolate other less benign interests in government information.

Surveys suggest that most constituents don't want the data collected by the government to be used for commercial purposes and it appears most people have been unaware that it has been used that way for years. One commercial vendor realized much of its multi-million dollar revenue in the previous year simply by packaging and selling drivers license data collected by its government clients to fewer than five commercial firms.

Concerns about privacy have already begun to escalate.

Example:

DoubleClick – the online advertising agency that has collected personal information through the use of cookies – found itself in the middle of a huge controversy when it was revealed that they could link names and addresses with web activity, including purchases, and make that

information available to advertisers. The Center for Democracy and Technology organized a protest and DoubleClick's advertiser's panicked. The firm's stock price dropped dramatically.

Earlier this year, the Supreme Court ruled, in *Reno v. Condon*, that the federal government, in addition to states, may regulate access to information gathered by the government. Previously it had been held that data in records collected by the state was regulated by the state. In this case, however, the Court ruled that once information crosses state lines, particularly as a commodity, it is subject to regulation by Congress. The Court's ruling may hamstring the states' ability to market public records.

The publisher of "*Access Reports*," a newsletter covering open government laws and information policy issues, recently wrote,

"Left to their own devices, the states and commercial information brokers would probably have exploited public records as a revenue source. But those times have probably come and gone, and the Supreme Court's decision opened Pandora's Box for federal regulation of state records."

One of the stumbling blocks to U.S. negotiations with the European Commission over safe harbor agreements has been the differing views of public records. Europeans believe that some kinds of personal information in public records should not be accessible to the general public and, in particular, to commercial interests. In a tentative agreement, the U.S. has agreed to the European position.

In 1999, President Clinton issued an Executive Order on privacy, which included an order to study the privacy impact on public records. The study is being undertaken by the Office of Management and Budget and it appears likely that it will support European concerns addressed in the safe harbor negotiations.

In May 2000, the Federal Trade Commission met and reviewed the status of the "self-regulation" approach that has been applied to online privacy. The Commissioners voted 3-2 to adopt a position that "self-regulatory initiatives to date fall short of broad-based implementation of effective self-regulatory programs," and "such efforts alone cannot ensure that the online market place will emulate the standards adopted by industry leaders."

Congress introduced more than 15 bills related to the protection of personal data in the past year.

FUNDING IN THE FUTURE

How will portal development and maintenance be funded in the future? Obviously no one knows and virtually any opinion can be justified and supported. It is certainly possible that the models that are attractive today in the first generation of portals may not be the same models followed in subsequent generations.

Meta Group, a market research firm headquartered in Stamford, CT, conducted surveys resulting in the conclusion that, by 2003/2004, payment for infrastructure, applications, and portal design based on transaction volume will be the preferred method for deploying e-government services in 70 percent of government jurisdictions with budgets greater than \$50 million. The surveys further indicated that jurisdictions with not only funding issues but also acute e-government skill shortages will outsource 90 percent of infrastructure, applications and portal design to government dot-coms or systems integrators.

Momentum Research Group surveyed 406 online businesses and citizens. Forty-seven percent of citizens said they would like to renew their drivers' license online; 38 percent said they would like to vote online; and 36 percent said they would like to access one-stop shopping for government services online. Seventy-five percent of citizens said they would prefer to access government services through a local or state government portal, rather than a federal government site. Of particular interest was their finding that more than 70 percent of citizens would prefer to pay a service fee than fund e-government initiatives through taxes. It is possible, however, that the respondents interpreted this to mean "new" taxes.

Steve Kolodney, Washington State CIO and past President of NASIRE, is among those opposed to making constituents pay additional fees to conduct government business online. "Our view is that the state shouldn't burden taxpayers with increased costs." (*Governing magazine, August 2000*) Kolodney supports giving discounts to constituents who enable government to reduce costs.

In the March 2000 issue of "*Government Technology*," Features Editor Tod Newcombe wrote,

"While some officials see nothing wrong with the self-funding model that is taking government by storm, others question the headlong rush into this new, and still unproven, form of electronic government. So far, none of the companies that offer these services is making any money. Should they succeed, there's no telling how the public will react when they hear about corporate profits being made by selling access to public data."

Anecdotal experience of some states supports the position that citizens will be sensitive to fees charged for online government services, and that citizens will be reluctant to use such services. There is some question as to whether the issue is one of the fee itself, or the fee size.

In a comprehensive 1999 study, the Texas Department of Information Resources reported there is really very little data about the real cost of e-government initiatives or cost-savings to be realized through implementation of portals and electronic transactions. This study concluded, however, that electronic government should not be positioned as a revenue generating program for Texas.

In all likelihood, a variety of funding models will ultimately exist and a preferred methodology may not emerge until electronic commerce in government has become much

more mature and both the private and public sectors have had an opportunity to assess the public's reaction to e-commerce and willingness to use it and pay for it.

When the answers to several questions become evident, the question of how to fund new and expanded portals and maintain existing ones will also be more easily answered:

1. Will the public be willing to pay convenience fees for a significant number of government services? If so, how much will they pay before they object?
2. If public response to the commercial use of personal data is significant enough, will it cause a redefinition of what is "public" and what is "private?" If there is a re-definition, will commercial firms no longer have access to data that makes their investment in government systems viable?
3. Will all vendors devoted solely to the electronic government market be able to survive financially while the public becomes accustomed to electronic commerce? If firms do not survive, will their government clients turn to other firms to bring those functions under government control?
4. If revenues from convenience fees become substantial, will governments elect to bring the electronic commerce functions under government operational control and retain those fees for themselves, rather than have them remain with the vendors?
5. As governments prepare to move beyond the initial phases of electronic government and require full integration of electronic commerce with back office systems, workflow and other labor saving functionality, will they expect transaction-based fees to pay for those improvements?

The list of questions can obviously be expanded, but these give a sense of those which can be accurately answered only after governments and their constituents gain substantial experience with electronic commerce.

DATA-SHARING

THE PROMISE

The promise of e-government is to make information and services more easily accessible and widely available. The web offers a convenient platform to access state services, since all that is typically required is a browser. It's easy to envision:

- A business or citizen signing onto a customized portal that provides specific information they want and links them to their most frequently used sites and applications.
- A custodial parent going online to see if the state has issued a child support payment yet, what the EBT balance is and what immunizations the child still needs.
- A child welfare worker checking on a juvenile's state-wide (or nation-wide) history of school attendance, treatment for mental illness, and trips through the juvenile justice system prior to placement in a foster home.

The current trend toward the portals as one-stop access points is compelling in its simplicity. Turning this promise into reality, is quite a different story.

THE REALITY

Well-designed web applications are deceptively simple. While new technologies are making the web a more powerful tool for interactive applications, web architects inherit many of the same barriers that have plagued client/server and mainframe application developers. Sharing data from multiple sources is a challenge that has become more fundamental as portal technology advances. The challenges fall into three categories:

- Revising business processes to accommodate a new model
- Managing technical complexity
- Overcoming data privacy and ownership issues

Creating new functionality using information from existing sources is technically complex. The following section identifies some of the challenges of data-sharing within the context of the planning phases of a standard software development methodology. These planning phases include:

- Business Objectives
- Functional Requirements
- Definition System Architecture
- System Design

The underlying assumption is that a strong investment in front-end planning will yield a better product in the end.

Business Objectives

Many technical projects fail because they have not been clearly defined in the beginning. A succinct definition of objectives from the business perspective will serve as an anchor for the project as it develops. For governments, business objectives typically relate to increasing service value and decreasing expenses, or making things run more efficiently.

Functional Requirements

Some questions to ask with regard to data sharing are:

- ***What business processes will be implemented or enhanced by this application?***

Many good business process methodologies exist that can be used to model web-enabled data-sharing applications.

- ***What data will be shared and what confidentiality requirements are there?***

As organizations move toward interactive applications, the clear delineation between what is public and what isn't becomes more blurred. For instance, the Center for Disease Control in Atlanta issues a form for doctors to report AIDS cases. The empty form is public, but the individual patient data is not.

Typically, aggregated, anonymous data is public, but person-specific information is not. Information on children, mental health, welfare and medical records would not normally be considered public information. The current emphasis in e-government planning as it relates to privacy and security should help define guidelines on what is public and what is private.

- ***Who will use the data?***

Defining who will be using the data helps address the business problems of confidentiality and access. With proper security and privacy controls in place, confidential data can be used for legitimate purposes. Some G2G examples are:

Distributed user bases, such as agency district offices or mobile employees.

Applications where information is shared with other entities, both public and private. This is becoming more common in employment, rehabilitation and training, and in human services applications, where the state contracts with outside vendors to coordinate and deliver services to clients. Law enforcement and agencies assisting juveniles have similar needs.

G2C and G2B examples include:

Any transaction using a credit card.

Accessing personal or business information held by government agencies.

- ***Who owns the data and how is it kept current?***

Portals are frequently designed to be clearinghouses for information residing in other places. If the portal's job is to provide links to other sites, data ownership is simple – the

entity that generates the data owns it and is responsible for its upkeep. This is a highly successful model, introduced by Yahoo and emulated in several states.

For data that is not defined as public, the barriers to sharing – either perceived or real – can be formidable. Some agencies may be prohibited by statute from sharing. Also, some federal agencies prohibit exchanging data over the Internet.

Solutions may include developing interagency coordinating teams, interagency data sharing agreements and memorandums of understanding (MOU). In some cases state statutes or county regulations may need to be changed.

System Design

Functional and business requirements are usually defined without regard to specific technology, so the next step is to assess alternatives and develop a system architecture and design. This is where the data sharing portion of an application begins to integrate with other components of the project, such as hardware platform, operating system, database, reporting, interfaces, network infrastructure and connectivity and security.

There are several technical options for data-sharing applications:

Data Warehousing

A data warehouse is a central repository for information, typically housed on an industrial-strength database on an enterprise server. For public data, the warehouse is an easy way to consolidate and present information using a web interface. Implementing a data warehouse containing confidential information requires additional design considerations for security and access permissions.

Selective data from participating entities would be transmitted to the data warehouse electronically on a predetermined schedule (nightly, weekly, monthly etc.), as required by users. The warehouse could be accessed via a secure Internet connection. A user permissions scheme would allow different levels of access. If the user community desired, standard reports could be defined. Data would also be available for analytical applications and ad hoc user queries.

Application Integration

This is a means by which data continues to reside in existing systems and is accessed using data broker middleware or a data interchange format such as eXtensible Markup Language (XML).

Data broker middleware tools are designed to translate data between different applications. They act as a “traffic cop” and translator between the Internet and the back-end systems that feed into them. This emerging technology holds much promise but can be costly and complex to implement.

XML is currently considered to be the universal data interchange format. It is an open-standards-based technology that is very flexible in its application. *(For more information on XML see: “An Introduction to XML’s Potential Use Within Government” NECCC, December 2000).*

Tiered Datasets

Tier 1 (Enterprise Core Data)

Tier 1 data represents the core data of the enterprise, common to all or most agencies. Tier 1 data is the heart of the enterprise referenced by all applications. There are two types of Tier 1 data – Lookup Tables and User Entities.

Lookup Tables:

- Static, rarely updated
- Maintained centrally
- Downloaded to applications from data warehouse – no “real time” access by agencies
- Users register to be notified of changes (explore automatic data replication)

User Entities:

- Dynamic, but infrequently updated
- Maintained centrally, by agencies or by users
- Available online or in data warehouse
- Provide “Identity”, “Standard” and “Enhanced” attributes to describe entities
- Distinguish different roles for entities (e.g. home owner or business owner) and for data attributes (home versus work address; shipping versus billing address) including the following:
 - Individual customers
 - Business customers and partners
 - Prospective businesses
 - Employees
 - Counties and municipalities (beyond standard lookup)

Tier 2 (Trans-Agency Affinity Data):

Tier 2 represents the extension of Enterprise Core Data stewarded by agencies. It consists of extended data sets describing attributes of Tier 1 entity interaction with agencies, owned by specific agencies but intended for sharing with other agencies, or for summarizing by entity. Data is dynamic, and is maintained by agencies or by users via e-government functionality. Tier 2 includes categories such as:

- Health & Social Care
- Public Safety
- Educational
- Administrative & Support
- Regulatory
- Economic Planning & Development
- Community (multi-jurisdictional)

Tier 3 (Programmatic Application Data):

Tier 3 represents application-specific data sets, owned and maintained by agencies. The Enterprise Data Model does not document or otherwise make this data available to

other agencies. Tier 3 data can be available to other agencies on an application-specific basis, but consideration should be given to migrating the data to Tier 2.

One of the realities of many data sharing and integration projects is a requirement that the systems producing the data must not be modified. A review of technical compatibility will reveal the extent to which systems are or are not compatible. Some things to consider are described in *Table 1*.

Some other activities in the design phase include:

- Proof of concept (POC) for user acceptance
- Process flow diagrams (online & batch)
- Database elements & structure
- User interfaces
- Rules engine or rules capability
- System access security
- User permissions structure
- Report layouts & content
- Interfaces to other systems

Table 1 - Technical Compatibility Considerations	
Criterion	Definition
Common System Architecture	Architecture refers to the overall blueprint and design of how the main parts and processes of the new system connect and communicate.
Common Hardware	Hardware determines the kinds of software that a system can use. Common hardware is relevant to compatibility in that the more similar the hardware the more likely it is that it can support specific operating systems and applications.
Common Operating System	An operating system is the program that manages all the other programs in a computer. Older applications may run on only one operating system, thus limiting their portability. Common operating systems affect compatibility in that they increase the ease with which information can be shared and possibly used by systems.
Common Database	A database is a collection of data that is organized so that its contents can easily be accessed, managed, and updated. The most common type of database in use today is a relational database. Most relational databases support a standard method of accessing data called Structured Query Language (SQL). Another key aspect of database compatibility is that it be Open Database Connectivity (ODBC) compliant. ODBC is a standard or open application programming interface for accessing a database. By using ODBC statements in a program, you can access files in a number of different databases.
Report generation	Systems display the information in their databases by creating reports. Reports are typically generated by software packages written specifically for that purpose, called report writers. Reports are either printed on paper or printed to a file. Systems that can create standard report files offer greatest compatibility because reports can be more easily transferred and read by other systems.
Network Infrastructure & Connectivity	There are many ways to transfer information among computers. Some examples are copying a file on PC to a floppy disk, attaching a file to an email message, and electronic interfaces between two systems to transfer files automatically.

Table 1 - Technical Compatibility Considerations	
Criterion	Definition
	Infrastructure refers to the physical hardware used to interconnect computers and users. Infrastructure includes the transmission media, including telephone lines, cable television lines, and satellites and antennas, and also the routers, aggregators, repeaters, and other devices that control transmission paths. It also includes the software used to send, receive, and manage the signals that are transmitted.
	Common capability and technology for transferring information improves the ease with which systems can share information.
System Lifecycle	Due to changes in required functionality and technology, information systems eventually become obsolete and are subject to replacement. A system that is young in its lifecycle uses current technology, is maintained with hardware and software upgrades and is expected to function for 5 - 10 years. Systems nearing the end of their lifecycle have obsolete, non-upgradable technology. A major change system update or replacement will impact compatibility between systems. The impact could be positive or negative.

Other Phases of the Software Development Lifecycle

After the design is completed, the new application progresses through development, testing & training and rollout. Since the details of these phases are entirely dependent upon the specific architecture and system design, they will not be addressed here.

Examples of Shared Data Applications

SilverSource Forms Clearinghouse – Nevada

The project objective is to make all government forms for public use available online through a web-enabled forms clearinghouse <http://silversource.state.nv.us/> linked to the state's main web page. Per the governor's executive order, the site was designed, tested and operational within 90 days of project startup.

The data sharing challenge was to provide access to forms from over 120 elected officials, agencies, boards and commissions. A design decision was made that forms would reside in only one place. If an agency already had a forms page, SilverSource would provide a link. If the agency had only paper forms, SilverSource would store them electronically its server. The effort included acquiring forms, scanning them and creating PDF files, then categorizing them. URLs for all forms already posted on state web sites were also documented. A database was designed that identified each government entity and provided a link either to the form site or to the PDF file. PDF files were housed in separate subdirectories on the SilverSource server. Additionally, keywords were defined to make searching more effective.

The design features a Yahoo-like interface that incorporates multiple ways to access data including searching by category, by agency or conducting a free-form search. Quick lists are also available for frequently requested forms. When a user clicks, an Active Server Pages is launched to deliver search results from a database. Clicking on the result opens a static (PDF) file or links to an agency forms site.

After almost six months in operation about 250 people visit SilverSource every day. The most popular ways that users look for forms are by clicking on a category, or using the search function or clicking on the “All Forms” button. Most popular forms are in Social Services, Vital Statistics, Ethics and Employment Security. Although the vast majority of referrals are from the state’s main web page, a search on Yahoo, AltaVista, Ask Jeeves and other search engines also provides access.

myNewJersey Portal – New Jersey

New Jersey is completing the initial development and implementation of its e-government technical architecture and production environment to facilitate the delivery of web-based services to citizens, businesses and employees of New Jersey.

The architecture provides for data, application and web hosting in a robust Unix-based 24/7 data center environment.

Additionally, the architecture will facilitate true portal functionality through the registration and management of intranet, extranet and Internet-based members into the myNewJersey Portal.

Management of portal members will be role based; i.e., users are assigned one or more roles (e.g., Basic Member, State Employee, Business Owner, etc.) which govern their access to informational and transactional services. Portal members are provided with a myNewJersey homepage, which they can customize with available content based on their assigned role(s).

The target member community during a pilot period will be from various communities including state and local government employees, as well as members of the general public and the business community.

The e-government architecture provides the following functional services:

- User registration, authentication & security services
- User customizable myNewJersey page creation w/role-based content channels
- Policy Management
- Directory Services
- ePayment services

- Enterprise Public Key Infrastructure
- Data, application and web serving platforms

Identification of the user, and assignment of a “role” is key to the effective use of the portal. All users must be registered, although the user does not have to be a state resident, employee or business operating in the state. A person may self-register with the portal, via the web, by supplying as little information as a name and e-mail address.

A role defines a group of users who share sufficient common traits to warrant the creation of a portal-based user group, with access to content and/or transactional systems specifically tailored to those traits or interests. All portal users will be assigned the default role of “member.” Users may also be assigned one or more additional roles.

Each “role” has an administrator who has the right to grant or remove an individual from that role.

Groups of users who share a common organizational interest belong to the same “entity.” Each time a user is assigned a role, that user/role is associated with an entity. For example, Jack is registered with the portal and has the default role of “member.” He is also a municipal clerk, so he carries that role as well. As the Municipal Clerk of Trenton, he can also be associated with the entity: Trenton.

Entities allow for decentralized user management, because there is always a manager for each entity in the portal.

Clearly, the use of roles and entities permit significant personalization for each user and facilitates sharing of information among individuals with common interests.

Closing Thoughts

While the concept of an enterprise portal is rapidly gaining acceptance and various forms of such portals are in design, development, and even early implementation, there really is not enough experience anywhere to allow organizations to benefit much from “best practices.” Indeed, the adopters on the classic “bleeding edge” of this technology have undoubtedly learned some lessons the hard way.

It is extremely likely that the portal landscape will change considerably over the next three to five years, as the public becomes more experienced with web-based transactions; as governments gain experience with critical issues of privacy, security and “public information” in a web-based world; and as funding models prove successful or unsuccessful.

While speed of implementation appears to be driving many government decisions, it is critically important that the government take the time to engage in serious planning, while evaluating the specific information and services that will be perceived as valuable by the public, and while considering the critical issues of financing, privacy and security. Further, it is essential for the organization to plan for benefits to the government, as well as to the citizen, through integration of the portal with an organization’s administrative systems.

Finally, every decision should be made with the clear understanding that there will be no opportunity to “turn back” when information and services are placed on the web. If one approach falters or fails, another must be readily available.

The public will quickly come to accept the new capability offered by a quality portal as an essential part of government’s service delivery.

Workgroup Members

Alia Mendonsa	Center for Digital Government	John Greaney	Dunn & Bradstreet
Ann Orlando	SAIC	John Kennedy	New Jersey
Bill Keip	Metamore	Joyce Murphy	Missouri
Bob Moriarty	SAIC	Judi Zito	Florida
Bob Sturm	NIC	Kara LaPierre	NIC
Brandon W. Lenoir	NECCC	Karen Helderman	Virginia
Brooks Knight	Texas	Lance Smith	Electro-net
Chuck Grady	Ariba	Mark Krysiak	Maryland
Dan Moore	CACI	Marvin Eicholtz	Montana
David Ancell	Michigan	Mary Alice Johnson	Digital Commerce Corporation
David P. Gragan	Oracle	Michael J. Corvino	SAP
Denise Lea	Louisiana	Michelle Sisler	AMR
Dick Ross	New York	Mike Peterson	CACI
Don Griffin	New Jersey	Miles K. Weigold	EMC2
Donald R. Greene	New York	Pat Kohler	Washington
Doug McCoy	EDS	Paul Weber	SAP
Douglas E. Boettner	Nevada	Paula Moskowitz	New York
Dugan Petty	Oregon	Peggy Fluman	Inacom Corp
Fred Norman	NIC Commerce	Ron Bell	Virginia
Gary Lambert	AMS	R.Thomas Wagner, Jr	Delaware
Helen McCain	Wisconsin	Randy Cole	IBM
Howard Freeman	3M	Richard B. Thompson	Maine
Jamie L. Spiegel	Texas	Richard Pennington	Colorado
Jan G. Cox	Idaho	Rick Wheeler	Andersen Consulting
Jan Heckemeyer	Missouri	Rob Duke	Surety Association
Jane M Wiseman	Andersen Consulting	Robert Attmore	New York
Jeannie Wood	Delaware	Robert Kirk	Illinois
Jeff Holden	South Dakota	Robert Smith	Wolfenet
Jeremy Starns	AMS	Robert Sturm	NIC
Jim Passier	Connecticut	Sandy Wright	Dun & Bradstreet
Jim Tucker	Way2Bid	Shannon Bisbee	AMS
Joan Daly	Civic.com	Stephen Lyon	IBM
Joan Sullivan	New York	Steve Sorett	Grant Thornton
John Bradley	Delaware	Theodore F. Winnie	New York
John C. Moore	Virginia	Tim Sheehan	Freemarkets
		Tom Jaworsky	Oklahoma