Online Government in Massachusetts

A Report of the Massachusetts Online Government Task Force

March 18, 1998

Commonwealth of Massachusetts
Executive Office for Administration and Finance
Information Technology Division

ONLINE GOVERNMENT TASK FORCE MEMBERS

Dan Greenwood Chair	Information Technology Division
George McCarthy	Division of Banks
Ray Campbell	Information Technology Division
Sarah Bourne	Information Technology Division
Jim McGillicuddy	Information Technology Division
Jim Belli	Information Technology Division
Roy Bean	Information Technology Division
Claudia Boldman	Information Technology Division
Christine Swistro	Office of the Comptroller
Gabe Gagliano	Office of the Comptroller
Timothy Landy	Operational Services Division
Larry McConnell	Registry of Motor Vehicles
Dimitry Petion	Secretariat of Consumer Affairs
John Shontell	Secretariat of Consumer Affairs

The Task Force would like to acknowledge the contributions of the Office of the Secretary of the Commonwealth, the Department of Revenue, the Center for Information Technology and Dispute Resolution of the University of Massachusetts, the Massachusetts Institute of Technology School of Architecture and Planning, and the Massachusetts Technology Collaborative. In addition, we are grateful for the many reviews and suggestions which served to improve the final report.

TABLE OF CONTENTS

Introduction

> *"The best way to predict the future is to invent it."*
> *- Alan Kay, inventor of the Graphical User Interface*

The Online Government Task Force was established by the Chief Information Officer to chart the immediate future course of online government in the Commonwealth of Massachusetts. The Task Force was commissioned to further define, research and evaluate these issues and to recommend a path forward to realize the promise of online government for the Commonwealth. Appendix A outlines the mission of the Task Force.

Information technology can reduce costs and enhance service quality of government when implemented correctly. In this context, "online government" means the use of network technologies that enable users to access information, people and processes.

Information includes the range of public records as well as data that a particular user has a right to access but that may be restricted to others. Access to people includes the ability to communicate with public employees. Processes includes business functions, such as filings, applications or payments as well as democratic processes, such as participating in meetings, hearings or even voting from a distance.

The emergence of the World Wide Web and web browsers has provided a simple yet powerful interface to networks of computers. This interface created an opportunity to open a wide range of government data and operations to users with unprecedented ease and effectiveness. However, opening government for online access requires analysis of several business, technical, legal and policy issues.

This report consists of two parts. Part I distills the research and discussions of the Task Force into a Vision for online government in Massachusetts, Guiding Principles and Recommendations for implementation. Part II provides more detailed background information and research conducted by the Task Force. The Current Status section provides information on the current technical environment, current department online government initiatives, legislative and policy initiatives, and industry and academic collaboration. The next section, Current Available Technology, gives the results of the Request for Information initiated by the Task Force and suggests an approach for analyzing security and authentication needs. The enclosed appendices provide more in-depth information about topics highlighted in the report.

PART I

Vision

> *"Virtually every public policy area is going to be affected in this new Information Age - from security, privacy, intellectual property, copyright protection, universal access to how bit flows are taxed across networks that largely ignore any kind of political border. Companies are going to invest and knowledge workers are going to move to those governments who create an environment where this electronic commerce can flourish."*
>
> *- Janet Caldow, Director, Institute for Electronic Government*

All business and interaction that can be performed at less cost and/or at a higher service quality if done electronically should be implemented online. This has been the guiding principle of the Online Government Task Force. The information age affords opportunities and risks. Some of the risks include: developing systems that can violate privacy interests, setting government policies that damage the growth of the young electronic commerce marketplace, or unwisely spending substantial sums of public money on technical solutions that are not based on business need or are otherwise wasteful. The opportunity is to embrace online technologies that enable better government. In this context, better government means:

Less:	More:
costly	efficient
distant	accessible
confusing	navigable
plodding	rapid
conflicting	consistent
error prone	reliable
bureaucratic	responsive

Efficient

Existing paper processes incur a range of cost, not all of which are obvious. Distribution, delay, archiving and access difficulties are all characteristic of paper-intensive work. Government is notorious for paper work, and Massachusetts government is no exception. Government has a duty to the citizens in general, and to the taxpayers in particular to eliminate waste, fraud, duplication and undue delay in public processes. Wise use of information technology to enable online government can serve the purpose of delivering legitimate government services at minimum cost.

While important, cost reductions are only part of the formula for a successful online government. When implemented properly, online government enhances the quality of service to citizens, businesses, vendors and others that interact with the state.

Accessible

There should not be a single public agency without a web presence of some kind. Eventually, every interaction and service should be available online in addition to, or instead of, the traditional paper form.

The Internet and World Wide Web have enabled access to services "on-demand." Accessible government is a key potential benefit of online technologies. To cite a simple example, it is reasonable to assume that the individual ordering fishing gear from L.L.Bean at midnight

might also want to obtain a fishing license from the Commonwealth - and so the demand is created for the same sort of convenient, flexible services from government as from private entities. Accessibility can be an even more fundamental tool for good governance when made available for people who can not physically come to the government due to distance, handicap or other obstacles.

Government on-demand will cause a transformation of the citizen/government, business/government, and government/government relationships. New networks for information access and feedback will be created where customization replaces standardization, business becomes streamlined - many services can be accessed via a common 'point of entry' rather than via numerous entry points, flat organizations replace hierarchies, timely feedback replaces long response times, simple processes replace complex, bureaucratic ones. With the essential pieces of the business, technical and policy structures in place, the state can become a collaborative inter-networked organization spanning state and local governments, schools, libraries, businesses, health care and other sectors. Services are delivered to citizens where they want it -- at home, at school, in the workplace, at public access points - anywhere.

Navigable

Once government services and other interactions are available online, another critical quality factor will be the navigability of those sites. The larger or more complex online interactions become, the more difficult they can be for a user to find, sift through and complete. Lack of adequate search engines or more sophisticated customer-focused navigation tools can defeat the entire online government enterprise.

Eventually some citizens will need to communicate with a live human. Online systems that allow users to communicate with personnel at an "electronic help desk" will also be necessary. Such online help desks can provide more robust tools for assisting users – including collaborative web browsing, assistance actually filling out online forms, avoiding simultaneous voice and data connections, etc. Navigational tools, including live help, will be important methods of delivering data and services that are simpler to locate and to understand in context.

Rapid

Unlike the paper-based counterpart, an online interaction can and should be more rapidly initiated and accomplished. The velocity made possible by online government should be carefully incorporated into the design and planning of each interaction so as to avoid choke points and needless delay at any phase of the life cycle of the interaction. Eliminating the paper from all phases of a given system can increase velocity.

Consistent

The transition to online government will further expose the inconsistencies among existing government activities as well as among newly created online systems. The act of making government available online creates a transparency that would not otherwise exist. The online interface of government must present a "single face" of government. Just as paving a cow path is not necessarily wise public planning, so too will it be important to revisit the assumptions and habits underlying current public activities as the online designs are being formed. This process must be done in coordination with all agencies so as to assure an online presence that is consistent with itself.

The risk of creating "government only" solutions that require installed bases or practices that are inconsistent with or, worse yet, in conflict with private electronic commerce practice is serious. Such a result would harm development of a critical Massachusetts and national market – the emerging electronic commerce marketplace.

A business or citizen who is deciding what electronic commerce tools to invest in should never be faced with a choice between general private commercial uses and different requirements to interact with government. However, if we continue to track closely with emerging standards and practices in the private sector, then government can actually enhance the growth of this market by making the value proposition even better for the person who uses electronic commerce tools because the tools will work equally for all their public and private sector needs. This ultimately redounds to the benefit of government as well, because it will make it easier for online government applications to be used less expensively and more widely.

Ultimately, the quality of serious online transactions will also depend on minimum base-line consistency among each level of government and between the public and private sectors. For example, the authentication, payment and interface requirements should not be in conflict.

Reliable

Though some reactively feel that electronic transactions are inherently less safe than paper-based transactions, in fact, when implemented soundly, the online system can be far more reliable. The ability to detect, and correct or flag errors is important. Data can be validated and entered automatically into databases to minimize the possibility of data entry errors. Similarly, appropriate levels of information security can reduce rates of crime and fraud perpetrated upon systems.

Responsive

Finally, online government can mean greater responsiveness and accountability by public servants to the constituency. The management and technical infrastructure should allow more direct communication and information flow with the constituent. To the maximum extent practicable, rigid and bureaucratic mechanisms should be designed out of the online government interaction. The process of interaction should permit more options and customization for constituent needs, treating the citizens like customers.

Envision the following scenarios

For the Business Partner of the Commonwealth:
Access key financial data - such as the status of a payment for a vendor, or the status of certain accounts - via a secure Web front end to a back-end system. Online payment methods are both accepted and available through the web. The risks of fraud and mistake are handled by security technologies settled by the partners through additional agreements specifying trade practices.

For an Organization Doing Business in the Commonwealth
All the forms, information and contact people associated with a regulation or a transaction with the government are available for process in one place and at the click of a button. You can track and manage the progress of your application or other transaction through the government process via online media. The forms, applications, correspondence, etc. are signed with a digitized signature device that combines biometric data with the document that invalidates the signature if any change is made in the document.

For a Citizen of the Commonwealth:
Finding out about meetings and hearings that affect you becomes simple and you can participate online without having to actually come to the State House or other government facility in person. You can communicate with public officials and staff directly in a virtual office setting. The citizen uses the same smart card, or public key digital certificate, or signature digitizer or any commercially standard security device that they use in private

transactions. The government solution requires no hardware, software or practices that differ from the citizens' existing installed base of security solutions.

How do we get there?

Realizing the vision will involve building a sturdy foundation. This foundation will have management and leadership components, policy components, and technology components. In addition, in order to fully take advantage of evolving technological capabilities and provide the highest levels of service in the new environment, leaders will need to take a hard look at how business is conducted today in order to identify how it might be improved.

The work that lies ahead includes:

- building a "trustworthy" infrastructure which assures authentication, integrity, confidentiality, access control and non-repudiation of transactions,
- creating the human infrastructure and service mechanisms to support the new "trustworthy" infrastructure,
- fostering more and better inter-organizational communication and collaboration (state-to-state, state to federal, state to local),
- creating a legal environment conducive to online government and eliminating regulatory barriers to electronic commerce,
- developing administrative controls which can be built into systems as simple rules and checks to replace traditional business controls which will be lost in automated information/transaction systems,
- ensuring new systems provide ubiquitous access, consistent interfaces and requirements ("one face"), ease of use, and are interoperable.

Guiding Principles

As we proceed to implement our vision of Online Government, our work should be guided by the following principles:

- Create no new regulatory or bureaucratic apparatus (eliminate existing apparatus where possible)
- Target initial resources toward the best business case for technology, not just the neatest technology
- Target security resources to what is needed for a given system - rather than the maximum for all systems
- Avoid direct competition with private sector providers of service or products
- Design and build solutions that promote a "single face" of government (at all levels of government)
- Implement solutions that leverage users existing private electronic commerce practices and technology
- Develop, organize and present online data and processes to suit the citizen or business, not government

The following section outlines specific recommendations in two general categories: Business and Technical.

Recommendations

Business

1. Develop a Web presence for every Department accessible via the Commonwealth MAGNet home page.

2. Increase agencies' Web presence by:

    2.1. Publishing major work products on-line

    2.2. Enabling customer inquiries on-line

    2.3. Handling core business transactions on-line, (i.e. Permits, Licenses, Filings, etc.)

3. Collaborate across agencies to:

    3.1. Identify and analyze common business practices

    3.2. Transform and centralize common business practices across organizational boundaries

4. Enhance communication and collaboration across agencies through:

    4.1. An online government Web site

    4.2. Tracking and publicizing department online government projects

    4.3. Common interest databases and discussion tools

    4.4. An interdepartmental online government project group that holds regular meetings to discuss issues, technologies and products, and best practices

5. Develop state-wide policies, guidelines, and legislation in the following areas:

    5.1. Privacy

    5.2. Management of Electronic Records

    5.3. Amendment of old " quill pen" laws

    5.4. Web-based revenue generation

    5.5. Security

6. Develop and implement a statewide coordinated authentication strategy to minimize costs and reduce risks to the Commonwealth through:

    6.1. The appropriate use of standards, including the safeguarding of privacy

    6.2. A framework for performing cost-benefit and risk analyses to compare PKI versus other security and authentication approaches

    6.3. Shared certificates and certificate policies

Technical

1. Develop Public Access infrastructure as an enterprise-wide baseline

    1.1. Publicize the current technical architecture and network security requirements

    1.2. Re-assess the current architecture and security requirements on an ongoing basis to support evolving Department needs and available technologies

2. Implement TCP/IP to desktops in all agencies to achieve:

    2.1. Adherence to a standard network protocol

    2.2. Adherence to an open system communication protocol

    2.3. Enable a standard client interface through the use of Web browsers

3. Develop a menu of Security and Authentication options to support various applications and transactions in conjunction with the development of Business Recommendations section 5.5 and 6.

4. Develop Application guidance that addresses at a minimum:

    4.1. ADA requirements

    4.2. Look and feel

    4.3. Site design

    4.4. Performance standards

PART II

Current Status of Online Government in Massachusetts

Background

As a result of two Information Technology (IT) bond authorizations in the Commonwealth of Massachusetts, the first enacted by the legislature in 1992, and the second enacted in 1996, IT development projects have been built and implemented by various agencies throughout state government to meet particular business needs. Some of these projects have brought services to a wider user population because they have been made available to users via the Internet and the World Wide Web. For example, the Registry of Motor Vehicles now provides a way for drivers to renew their vehicle registration or pay fines via the RMV Web site. While these IT investments have been successful for their particular organizations, over the last year, attention has begun to focus on how to leverage the growing number of online, automated systems and the maturing Internet-based service capabilities to create a more comprehensive vision of integrated, online Government services via the Web which cross organizational boundaries.

Certain agencies in state government have gained substantial experience with online systems development and new technology deployment. The Commonwealth's Chief Information Officer, Louis Gutierrez, decided to tap that growing knowledge base to create the Online Government Task Force. The Task Force was charged to help chart the immediate future course of online government in the Commonwealth by defining a vision for online government, assessing the current environment (from both a technical and a policy/legal standpoint), identifying emerging common applications ripe for Internet and Web implementation, reviewing currently available technology offerings of interest, and then reporting on our findings and making recommendations for further action.

The Task Force began by identifying and evaluating applications with varying security and authentication requirements, which were used as examples to frame a Request for Information (RFI) on products and services to meet these needs. The information gained from that RFI is detailed in this report and will inform the Task Force's findings and recommendations. The Task Force also conducted a survey of existing and planned online government projects throughout the Commonwealth. This survey provided an indication of current online government initiatives that are deemed important by agencies.

Internal Current Computing Environment

MAGNet, the Internet and Current Public Access Architecture

The Commonwealth of Massachusetts' internal network is called MAGNet, short for Massachusetts Access to Government Networks. It is a TCP/IP routed network, utilizing 245 Cisco routers strategically located throughout the Commonwealth. MAGNet provides 151 State agencies with high-speed frame relay, centrally managed connections. This network allows agencies to access many Commonwealth resources including the mainframe systems and the Information Warehouse and also provides the capability for interagency communication. TCP/IP has been implemented in approximately 60% of the Commonwealth's agencies to date.

Local Area Networks (LANs) in the Commonwealth currently run several operating systems, including Windows NT, Novell NETWARE and Banyan Vines operating systems. The current Commonwealth standard stipulates at a minimum Windows NT Server Version 4.0, Banyan VINES 6.3 with TCP/IP Server-to-Server Option for remote TCP/IP access and Novell NETWARE Version 4.1 with TCP/IP Option(s) such as Novix or LAN Workplace.

The current desktop PC standard for new purchases is a 200 MHz Pentium processor with 32 MB memory and a 10/100 MB Ethernet network interface card. The operating system is 32-bit Microsoft Windows (either Windows 95 or Windows NT 4.0 Workstation) with an Internet Web Browser (either MS Internet Explorer 3.0 or higher or Netscape Navigator 3.0 or higher).

GTE/BBN and MCI provide Internet access, with high-speed connections to MAGNet through the ITD Network Control Center. Security is maintained via a firewall, through which all traffic to and from the Internet passes. Internet users can be securely connected to network resources within MAGNet via specially configured and protected servers. Commonwealth agencies can obtain additional information about the current Public Access Architecture by contacting the Information Technology Division.

Commonwealth of Massachusetts Web Site

The Commonwealth of Massachusetts web server is home to web sites for eighty state agencies and handles 3 million file requests monthly. The Internet Services Group within the Information Technology Division provides consulting services and training to state agencies as well as server space at no cost. An average of three agency web sites have been added each month over the past two years. Unfortunately, many agencies and other public entities still have no web presence on the state web site.

Through the state's web site, agencies have been able to make their information available to a wider audience without the incremental costs associated with paper distribution. The state web site has been the source of publishing "firsts" for the Commonwealth: the Comptroller's financial statements, the Governor's budget recommendations, employment statistics, and local aid announcements are among the materials that can be found on the web when or before a paper copy is available. As discussed later in this report, agency sites are beginning to go beyond publishing to more interactive applications such as accessing bid solicitations and renewing automobile registrations.

X.500 Directory Server

The Commonwealth possesses an X.500 Directory Server. X.500 is not a database (though it may use one). In its basic definition X.500 is a technical architecture for constructing a directory service according to a defined set of standards.

The directory itself is a hybrid repository/index/pointer to objects. "Objects" is meant in both the data and physical sense (the data may at times point to a physical location). Standardized X.500 data object classes define the directory entries by specifying which attributes can and must be associated with each particular object class for entries assigned to a particular object class.

The "authoritative" source of the directory information is typically maintained elsewhere - but is loaded into the directory, with appropriate mapping of entries to X.500 object classes/attributes, for centralized "normalization"/access to that information. Multiple sources may be used in combination to construct entries. Given this positioning of the technology, following are some examples of how X.500 can be used:

- White Pages—for e-mail addresses, URLs, Postal Address, employment/employee information, all types of public resource information (including recreation information, assistance programs, government policies, etc.),
- Public Key Infrastructure support (X.509/LDAP, in particular) to store and manage user authentication certificates,
- Interface to Smart Card ID cards with all applicable applications of such, e.g., authorizations, building security, registration/enrollment purposes,
- For application program reference, e.g., CommBridge.

Keeping in mind that since the directory is a repository of "pointers"/"indexes" and not the "authority", information can be made available to people/applications without jeopardizing or compromising the source systems. Multiple images of the directory can be constructed so that depending upon authorizations a subset of information is available for query. Internet technologies - Web and LDAP, in particular, provide the access mechanisms to the information. However, within the Commonwealth, at this time the dominant use of the technology has been with E-mail.

The Comm-Bridge project provides the internal framework for secure, authenticated application to application level communications within the state network. This system uses public key certificates to authenticate applications and devices on the network.

Current Online Government Initiatives

Agency Projects

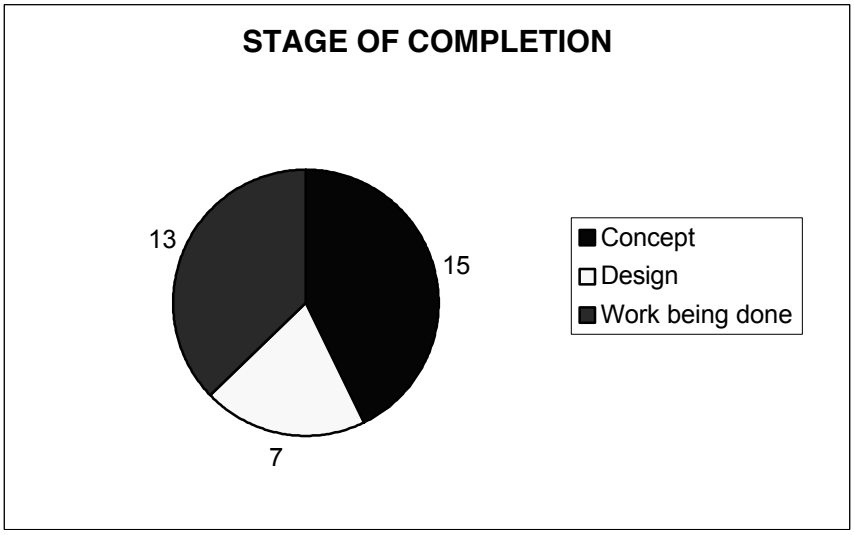
The Task Force conducted an investigation of current online government initiatives within the Commonwealth. As part of this investigation, the Task Force drafted a survey which was distributed to each executive branch agency and other segments of government. The survey questions were designed to ascertain the scope, security requirements, payment features and stage of completion for each initiative.

The table below indicates the short project description and the agency involved with each application. A total of 35 projects are listed.

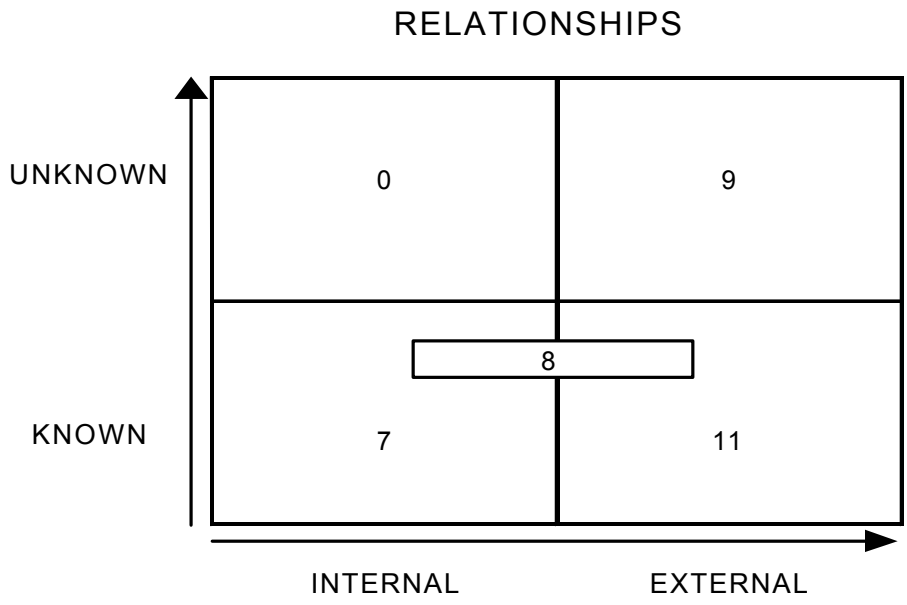
Agency	***Project***
Bureau of Special Investigations	Investigator's System
Campaign and Political Finance	OCPF Web site
Committee For Public Counsel Services	PC BILL
Department of Correction	Inmate Research Statistics project
Department of Housing and Community Development	Client and Fiscal Management System (CAFMIS)- IT2
Department of Revenue	Tax Exempt/Resale Certificate Verification
Department of Revenue	Corporate/Personal Income Tax Extensions
Department of Revenue	Customer Feedback Form
Department of Revenue	Electronic Funds Transfer (EFT) Application
Department of Revenue	Taxpayer Change of Address Form
Division of Banks	Authenticated Internet Forms Filing
EOHHS	Client Index
Executive Office of Environmental Affairs	Internet Access to GIS
Executive Office of Public Safety	Public Safety's Non-Confidential Information
Fisheries, Wildlife and Environmental Law Enforcement	SPORT
General Court	Massachusetts General Laws Online
Holyoke Community College	Student registration over the Web

Agency	*Project*
Holyoke Community College	Student access to personal information
Mass Highway	Incident Management
Mass Highway	Federal Highway Electronic Data Exchange
Mass Highway	Traffic Video Information
Mass Highway	GIS Map
Massachusetts Aeronautics Commission (MAC)	Airport Information Management System (AIMS)
Mount Wachusett Community College	Distance Learning
North Shore Community College	EDE
North Shore Community College	State SQL server for spending plan
North Shore Community College	Banner Web for Student
Office of the Comptroller	MMARSWeb/ManagerMMars
Office of the Comptroller	MMARSWeb/VendorWeb
Office of the Comptroller	MMARSWeb/WEBWarehouse
Operational Services Division	Procurement Desktop
Operational Services Division	Comm-Pass
Registry of Motor Vehicles	Express Lane
Secretary of State	Voter Information
Worcester State College	Colleague INTERNET Access

A copy of the Survey and cover letter as well as a more detailed spreadsheet containing the survey results can be found in Appendix B. The following charts provide an analysis of the results in certain key areas:

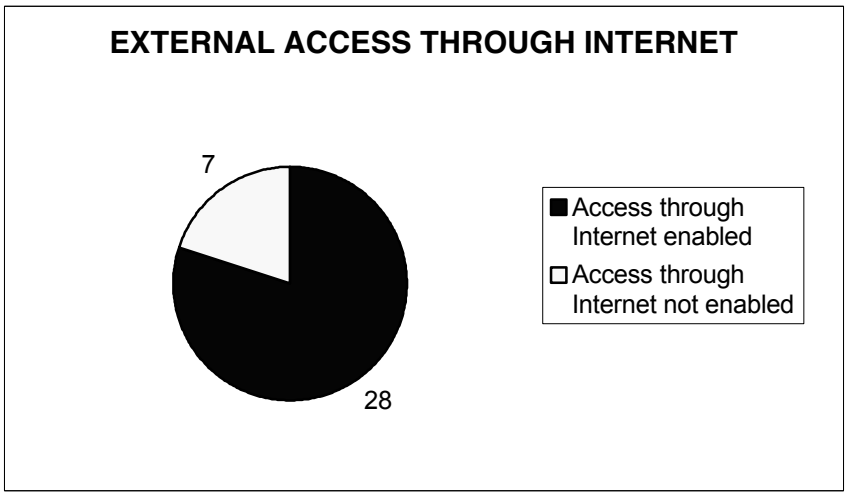


While the majority of Department projects are still in the Concept or Design stage, it is significant to note that work is already being done on 13 projects.



The chart above categorizes the projects according to the relationship between the agencies and the target audiences for the applications. This relationship is a key determinant of the level and type of authentication that will be needed for individual applications. The term "internal" is used to encompass entities within State government and its agencies such as employees. "External" is used to refer to entities outside of State government such as vendors and citizens. "Known" entities are those with whom the Commonwealth has a previously established relationship such as contracted vendors and service recipients. "Unknown" entities do not have existing relationships with the Commonwealth such as an anonymous member of the general public or a new vendor responding to a solicitation request.

The majority of projects (26) involve **known** internal or external entities or a combination of both. Only 9 projects involve unknown external entities. However, most of these applications involve the provision of public information for which authentication would not be necessary. The need for authentication will vary based on the particular application and will depend on an evaluation of the risks, the benefits and the costs of levels of authentication. In the case of known parties, we assume that authentication will be easier to implement because of existing agreements, communications or other available methods of identification. Likewise, authentication should be easier to implement with internal parties than with external parties.



The majority of applications (28) may be accessed by external parties through the Internet. Many can also be accessed within the state's Network (MAGNet).

Some of the online government applications deserve special consideration. These "killer apps" are examples of the new model for delivery of state services:

The Division of Banks

Each week the Division of Banks (DOB) publishes a *Consumer Credit Guide*. To qualify for inclusion into the weekly guide a participant must be a licensed mortgage lender or a state or federally chartered financial institution and the Division verifies that each entity is in fact able to participate. DOB is piloting a new process whereby, instead of a manual, FAX-based procedure, banks use the Internet to access DOB's Web site. The DOB pilot attempts to create authentication using an X.509v3 public key certificate. They will use this authentication to enable banks and other financial institutions to report and attest to their interest rates (file forms) with the Massachusetts Division of Banks over the Internet and be assured that the Division of Banks has accurately received and recorded the information. At the same time, DOB will be assured (via the certification authority) that the reporting institutions are "authentic" (legitimate) and will have the digital signature of the financial institution as a record of the completed transmission.

The Registry of Motor Vehicles

The Registry of Motor Vehicles (RMV) has a series of online transactions available on the Internet. Using SSL2 security, the RMV accepts credit cards as payment for citations, registration renewals, ordering a special plate, and requesting a duplicate registration

certificate. SSL2 was used for these RMV transactions because they require only confidentiality and not authentication (SSL2 does not provide authentication). Over 32,000 people have taken advantage of this new form of government access since July 1996. Additionally, ordering vanity plates, requesting driving history, and reserving road exam test time will soon be available.

Operational Services Division

The Operation Services Division (OSD) has launched Comm-PASS (Commonwealth Procurement Access & Solicitation System) which is designed to advertise solicitations (RFRs) on the Internet. The system has the capability to both advertise the existence of the solicitation and distribute it by allowing the user to download the solicitation files. The system is available 24 hours a day, 365 days a year. A department can advertise a procurement and distribute the bidding materials as files. This allows the department to save on printing and mailing costs. The department must also post the result of the procurement (who bid, winning bidder, etc.) in Comm-PASS. This allows the vendors to know who won without calling the procurement staff, saving both parties time.

Legislative and Policy Issues and Initiatives

Some of the major policy issues facing the Commonwealth with regard to the deployment of Online Government and Electronic Commerce revolve around authentication, privacy and the fairness of information practices related to the creation, storage, use, modification, disclosure and destruction of electronic records that personally identify an individual or contain otherwise sensitive data. The extent to which authentication is required in the first place is itself a policy – not a technical – issue.

The ITD Office of the General Counsel has worked on several privacy issues related to electronic records systems for the Commonwealth. The Deputy General Counsel for the Information Technology Division has testified before Congress on issues of electronic data privacy (written testimony available at: http://www.tiac.net/biz/danielg). The Commonwealth should not require authentication of an individual where it is not necessary to accomplish the underlying transaction.

For example, there will be situations where the Commonwealth has no direct interest in the individual who conducts a given transaction, but does need assurance that the user is authorized or maintains a particular role within an organization. Similarly, there may be a place for pseudonyms or anonymous transactions where appropriate. If authentication occurs, then the Commonwealth should assure that the personally identifiable data is kept in accordance with fair information practices guidelines and is treated with the highest appropriate care. More information on the privacy and fair information practices issues presented by electronic authentication and records systems is included in Appendix E of this document.

The Commonwealth must also grapple with the extent to which we permit private sector parties to create, manage, sell or otherwise control public information that is in electronic form. Some states have "out-sourced" the management of their official web sites, for example. In such arrangements, the private sector vendors will typically cover costs and create profits by selecting some data or processes to withhold from the public unless a subscription or other fee is paid to the vendor. This subscription may be for so-called "value added" data or services, such as online transaction systems that the vendor provides to state agencies. It remains to be determined whether such arrangements would be in the public interest or would risk over-commercialization of processes and data which would otherwise be free for public access.

Another area of concern relates to the accessibility of online resources to all citizens. As mentioned earlier, a key potential benefit of Online Government will be the easier accessibility of data to the public. However, the government, as an organization that is accountable to all the people, must also consider the equity of making data or resources available online when many citizens still do not have access to computer resources. Furthermore, the Americans With Disabilities Act (ADA) must also be applied to all online resources to assure handicapped citizens are not unduly disadvantaged by the presentation of data via online methods that can not be accessed due to disability (such as blindness). More information is available on how to assure online government compliance with the ADA in Appendix E of this document.

Underlying all these policy concerns is the more fundamental principle of governance. It is the citizen's constitutional right that their government be accountable to the governed at all times and in all activities. Using online government to reduce costs and enhance service quality serves the deeper purpose of maintaining high levels of responsiveness and accountability to the self-governed.

Proposed Massachusetts Electronic Records and Signature Act

One of the factors slowing more widespread use of the Internet for government transactions is the legal uncertainty surrounding the use of electronic media rather than traditional paper-based systems. For example, a search of the Massachusetts General Laws reveals over 4,500 sections that refer either to written documents or signed documents. This has generated substantial uncertainty as to whether an electronic transaction will have binding legal effect.

To address this uncertainty, the Information Technology Division, at the direction of the Executive Office for Administration and Finance, has been working to draft legislation that would confirm the ability of state agencies to use electronic transactions even when there is a law requiring a written or a signed instrument. The Massachusetts Electronic Records and Signatures Act (MERSA) is designed to validate online government without forcing agencies to abandon paper-based systems until they are ready to do so. A copy of the latest version of MERSA is available on the ITD legal department's web site (http://www.state.ma.us/itd/legal).

In brief, MERSA states that where any law requires a writing, that law is satisfied by a "record." The statute defines a record as "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form . . . [including] electronic records and written records." Regarding signatures, MERSA provides that where any law requires a signature of a person, that requirement is met by that person's electronic signature. In addition, MERSA explicitly states that agencies "may create and receive electronic records in lieu of written records, and may also convert written records to electronic records." Realizing that not all agencies are ready to support electronic transactions, MERSA provides that nothing in the statute shall be construed to require any agency to use or permit the use of electronic records or signatures. MERSA also enables non-governmental electronic commerce transactions between private sector parties. However, nothing in MERSA would change or limit existing consumer protection provisions of law.

While several states have already adopted so-called "digital signature" laws, MERSA represents a new approach that is rapidly gaining favor with other states. Unlike the first digital signature law enacted by Utah, MERSA is "technology neutral" in that it does not specify the type of technology that parties must use to gain the benefits of the law's provisions. In addition, MERSA is non-regulatory, whereas Utah-style laws impose stringent licensure requirements for certain companies that provide services related to digital signatures. A recent Internet Law and Policy Forum study of state electronic signature legislation shows that the trend among states adopting such laws is distinctly toward the Massachusetts approach.

Relationship with Other States and the Federal Government

The Commonwealth has collaborated closely with the National Conference of Commissioners on Uniform State Law on the drafting committee for the Uniform Electronic Transactions Act (UETA.). In addition to the Commonwealth's formal committee membership, the Information Technology Division has actively assisted the UETA drafters, based on MERSA. As a result, official comments to the UETA cite MERSA in several sections. The Information Technology Division, through the Office of the General Counsel, has also been involved in Electronic Commerce legal reforms within other states and state organizations. The Deputy General Counsel (DGC) for ITD has formally testified or presented on these issues before the National Governor's Association, the Western Governor's Association, the states of Rhode Island, Tennessee, West Virginia, Mississippi and other venues.

The Commonwealth has also been a leading coordinator of the federal-state relationship on these law and policy issues. Governor Weld joined the United States Innovation Partnership – an initiative of the National Governor's Association and the White House Office of Technology Policy created to coordinate technology policy at the national level between states and the federal government. The DGC has served as the USIP Governor's Alternate under the Weld and Cellucci administrations. In this organization, the Commonwealth has led development of an experimental Internet web site for collaborative discussion of electronic commerce law and policy. The web server is hosted at the University of Massachusetts and is used by state and federal policy makers in both the executive and legislative branches as a two-way communications and update tool.

The DGC has testified before the Senate and Congress on multiple occasions as federal legislators seek information and direction on electronic authentication and data privacy legislation. The written testimony is available at www.state.ma.us/itd/legal. As part of this cooperative posture with our federal partners, the Office of the General Counsel has also assisted Congressional staff with the drafting of federal bills, including H.R. 299, the "Electronic Commerce Enhancement Act of 1997." Specifically, the DGC's contributions led to provisions in the legislation that assure the technical standards for federal government electronic forms "shall be compatible with standards and technology for digital signatures used in commerce and industry and by State governments." This language directly reflects the Commonwealth's position of supporting and using private sector technical standards in government operations and policy. The DGC has also presented at federal agencies, such as the "Access America" conference of the National Performance Review, and the "Public Forum on Certificate Authorities and Digital Signatures" by the National Institute for Standards and Technology. In addition, the DGC has consulted with federal policy makers regarding electronic commerce issues, including Ira Magaziner, Special Advisor to the President of the United States.

Industry Collaboration

The Certificate Authority Ratings and Trust Task Force of the Internet Council

Late in 1996, the Office of the General Counsel of ITD, in conjunction with the Office of the Director of the Digital Signature Program for the State of Utah, agreed to organize a meeting to discuss the creation of general market based accreditation standards for use of digital signatures and Certificate Authorities. Soon, Carolyn Purcell, CIO for the state of Texas and then President of the National Association of State Information Resource Executives agreed to take the leadership for pulling this meeting together. The meeting was attended by several states, U.S. Federal agencies, representatives from several countries, every major Certificate Authority, IBM, Microsoft, Netscape, National Computer Security Association, Novell, Open Market, Deloitte & Touche LLP, the Massachusetts Technology Collaborative, Telecom Ireland, Stanford Law School's Law and Technology Policy Center, and the United States Council for International Business.

By the end of the collaboration, three state associations—the National Association of State Information Resource Executives (NASIRE), the National Association of State Auditors, Comptrollers and Treasurers (NASACT), and the National Association of State Purchasing Officials (NASPO) -- and their state government members had assumed a coordinated leadership role on this issue. The three associations agreed to work through membership to the Internet Council of the National Automated Clearinghouse Association (NACHA) as an open and participatory private sector based forum within which to grapple with these issues. In this forum, the states are working with Federal government and private sector representatives to develop a market-based means to evaluate or rate the trustworthiness and performance of certification authorities issuing digital certificates as part of a PKI-based electronic commerce solution. As of the publication date of this report, some 14 state governments are paid-members participating in this effort. The initiative is taking place under the Certificate Authority Ratings and Trust Task Force (CARAT) of NACHA's Internet Council.

The CARAT Task Force is working on the development of market-based rules and standards for the evaluation and rating of certification authorities and the certificates they issue. For PKI to be truly useful as a serious business tool, subscribers, relying parties and the general public must have confidence that CA's will be held accountable for their performance and services, with appropriate liabilities established. However, a trustworthy system must also take into account the rights and responsibilities of the other parties involved.

Through participation in the ANT Work Group's CA pilot, and research and collaboration with other industry and government efforts related to CA accreditation and evaluation, CARAT task force members are striving to develop a uniform regimen of metrics, processes and standards (operating rules or "named policies"). These named policies would support the use of registered certificate policies and specified types of transactions conducted on open networks and supported by an "open but bounded" public key infrastructure (PKI), usable by both private sector and government organizations. A related intent is to use the certificate policies as the basis for a controlled test of service applications in a real operational setting among public and private sector members of the Internet Council.

Academic and Educational Collaboration

The Information Technology Division hosted a public briefing by the National Research Council on their report: "Cryptography's Role in Securing the Information Society." The briefing was held at the Gardener Auditorium in the State House on Wednesday, August 7, 1996. Co-sponsored by the Boston Bar Association's Computer Law Committee and the Boston Computer Society Legal Group, this briefing brought together members of the academic, financial services, government and technology sectors of Massachusetts to discuss national cryptography policy and the role of state government. This was an example of state government acting as a convener of major policy debates in a public, non-partisan forum. More information on this event is available at http://www.tiac.net/biz/bcslegal/nrc1.htm.

The Commonwealth of Massachusetts and the Massachusetts Institute of Technology have cooperated to explore technical, design and policy issues in an academic setting. The Deputy General Counsel for the Information Technology Division holds an academic appointment as lecturer at MIT, where he teaches at the graduate level on topics of electronic commerce, virtual communities and online government. In 1997, the graduate course: "Virtual State House" generated several working prototypes of virtual reality, multi-user online government environments. In the Spring of 1998, the graduate course: "Designing Electronic Commerce and Online Government" is exploring the relationship between technology and policy in the design and implementation of online transactional systems.

Current Available Technology

> *Excerpt from: "States' Role in Developing Digital Signatures Policies and Standards"*
>
> *States, like other levels of government, have an interest in the promotion of electronic commerce. The government at all levels has a duty to seek efficiencies in the delivery of government services by reducing costs and enhancing service quality. Modern economic development policies should specifically promote electronic commerce in the private sector. Digital signatures are an important tool to enable secure electronic commerce and the technology underlying such signatures requires special attention.*
>
> *- Statement by the Legislative and Policy Work Group of the Information Security Committee of the American Bar Association, 7.31.97*

The Task Force investigated several technologies with an eye toward solutions that are cost-effective and which meet our business needs for implementing systems that are simple and efficient for the user. Much of the attention of the Task Force was focused on information security technology, and particularly on implementations of public key cryptography. The use of so-called digital signatures was a major issue. Please see Appendix D for more information on Electronic Authentication.

Topics discussed included: how the key and certificates should be generated and managed; to what extent, if any, should the Commonwealth act as our own Certificate Authority (CA), what existing business lines would benefit from use of digital signatures, how would various CA's certificates be handled technically by the Commonwealth, what criteria will the Commonwealth use to determine which CAs will be deemed sufficient for a given transaction, and what policies would promote the broadest use of the fewest certificates by a citizen with agencies.

The Task Force determined that it is too early to definitively decide these issues because this entire area is still maturing. These issues are also the topic of discussion at the federal, state and private sector levels. Efforts are underway to pilot new technologies and coordinate efforts to ensure the interoperability of approaches. The Commonwealth needs to continue its involvement with these various groups and continue to identify Department requirements with the goal of articulating a coordinated statewide approach.

Technology Matrix

The Task Force issued a Request for Information (RFI) to vendors with the goal of seeking information on products and services that will enable the Commonwealth to use the Internet and internal networks for secure messaging and transactions. The RFI document is included with this report as Appendix C.

The RFI elicited a number of responses, ranging from descriptions of available technology to offers of integration and planning services. The RFI responses are summarized in the following matrix. Complete RFI responses are available for review at ITD.

RFI Respondent	Product/Service Description	What does it do?	What does it cost?
Andersen Consulting	PLANNING SERVICES Andersen provides no specific products or solutions in this response. They offer several strategies for providing secure Internet services. To provide specific solutions Andersen requests further information regarding the Commonwealth's security policies.	This response provides overviews of the latest Internet security systems (hardware, software, and services). Andersen needs further information from the Commonwealth including security policies and hardware requirements.	No specific costs are discussed. The response states if the Commonwealth selected Andersen as a "full-solution partner", instead of disparate hardware and software vendors, the implementation of on-line government would be cost neutral.
BBN Planet	SERVICE BBN proposed several ideas for specific solutions for the Commonwealth. BBN proposed the use of encryption technology, SecureID cards, and SSL public key exchanges among other approaches.	BBN's solution will incorporate 4 qualifications for secure electronic transactions: 1) user is certain of communication with correct server. 2) server is certain of user identity 3) information transmitted is kept between user and server 4) user and server can be certain information does not alter during transmission process.	No specific costs were provided. BBN will provide another proposal when the details of the particular application are known. BBN requires use of commercial web browsers and can recommend proper software.
Control Data	COMBINATION: PRODUCTS & SERVICE Control Data offers a combination of their own x.500 directory along with technology from Entrust (see above) to provide secure web-based electronic commerce.	Control Data's security technology includes digital certificates to authenticate users and protect the desktop; public key cryptography and virus protection to safeguard messages; and firewall and virtual private network management for network security. All features can be integrated into the X.500 system now being used by the state.	No specific costs provided.
EDS	SERVICES EDS offers the ImagineCard solution. ImagineCard is part of EDS' HP Praesidium Enterprise Security Framework.	The ImagineCard solution combines smartcard technology with the latest advances in public/private key cryptography to provide strong security for electronic transactions. ImagineCard is a component of the HP Praesidium Enterprise Security Framework offering several security products to lessen the risk of doing Internet business.	EDS mentions situational costs. However, without further specifics they cannot craft complete solutions with associated costs.
Entegrity Solutions	PRODUCTS Products offer a series of services: *NotaryPlus* provides CA framework. *AssureWeb* provides access control. *SignOn* provides authentication for the entire	Entegrity's products provide proper authentication, access control, privacy and non-repudiation needed for all secured electronic transactions. This combination of products allows the	Solution requires about $30,000 of server based software. Client side software and support is $36. Certificates per-issuance will cost between $2-3.

RFI Respondent	Product/Service Description	What does it do?	What does it cost?
Entegrity Solutions (cont.)	session. *Mailer* provides encryption/decryption. *Security Development Platform* provides integration for all aspects of security system.	Commonwealth to become their own CA or they can enlist a separate service.	
Entrust	PRODUCTS Entrust offers security products, public key infrastructure, and key management architecture The products are X.509 based.	Entrust offers a full range of public key infrastructure products and system solutions. Entrust recognizes the cycle of a key across the enterprise system and ensures its compatibility.	Costs estimate for server hardware is $6,000 per 5000 users. Client licensing costs are $159 (negotiable) per user.
GTE	SERVICE/PRODUCTS GTE offers deployment of enterprise-wide authentication and access control systems using X.509 digital certificates. GTE Cybertrust is the certification authority.	GTE offers Enterprise Information Access. By using GTE CyberTrust to generate X.509 certificates, they are able to provide secure and authenticated Internet access.	No specific costs were provided. Client will need a PC web browser. Central web server hardware and software are required. The Commonwealth can buy a CA server or use the services of GTE. GTE identifies that the main cost will be in system integration.
IBM	PRODUCTS IBM offers security products and certification authority services. IBM also provides authentication and encryption based on X.509 certificates.	Strategy relies on access control lists for application, transaction and data security. The IBM Vault Depositor server can support both persistent and non-persistent Web-to-host connections.	Hardware and software purchase required. Solution costs not provided in response.
KPMG Peat Marwick LLP	SYSTEM INTEGRATION SERVICES KPMG outlines their own "solution architecture" using numerous technologies. The core of their offer however is consulting services.	Their solution architecture uses firewall technologies to separate the public Internet from the internal networks of the Commonwealth with a "demilitarized zone" (DMZ). Servers on the DMZ provide user authentication, user access restriction, and bind users to their submissions.	No specific costs provided.
N*Able	PRODUCTS N*Able offers enabling smart card technology for the Secure Electronic Transaction (SET) standard.	Product is a low-cost smart card to hold private certificate and credit card information. Technology relies upon digital certificate to secure a transaction. Cards are designed for usage with the SET protocol to facilitate transactions between consumers and merchants. Card scanning device for PC necessary.	N*Able smart cards are offered in range from $2.00 to $25.00.
NetDox	SECURE TRANSMISSION SERVICES NetDox offers a pay-per-	Characterized as an "Assured Electronic Information Delivery	Costs include a per-message charge of $6.85 for packages up

RFI Respondent	Product/Service Description	What does it do?	What does it cost?
NetDox (cont.)	use service designed to assure the security and confidentiality of electronically transmitted "packages" created by the sender.	Service", the NetDox server handles and assures all transmissions. NetDox offers a wide range of security and non-repudiation services for documents, images and video with varying levels of security.	to 250Kb. Additional charges pertain to larger messages, message confirmation, and longer term record archiving.
Oracle	PRODUCTS Oracle provides X.509 certification, Kerberos and other single sign-on technologies.	Available products support secure access through non-Oracle firewalls and persistent/ non-persistent database connections behind firewalls. Security server CA technology available.	Server hardware and Oracle software is required. Incentive pricing is mentioned in response but not clearly defined.
PenOp	PRODUCTS PenOp is software for the secure capture, management and verification of handwritten signatures.	PenOp enables users to perform a normal autograph and have it captured electronically. PenOp can also reliably capture, store and transport signatures between different systems. PenOp does offer signature verification.	PenOp offers run-time licenses costing $100 to allow signature captures on workstations. The digitizer pad and pen required to perform the signature cost around $100. For signature verification, the price goes according to the enterprise scale. PenOp SDK costs $699 + $20 shipping.
Trusted Information Systems (TIS)	PRODUCTS TIS offers security software, including the Gauntlet Internet Firewall, the Gauntlet PC Extender and SmartGATE: Guaranteed Authenticated Transaction Environment.	The Gauntlet Internet Firewall provides secure access and communications between private and public networks. The PC Extender creates a secure virtual private network (VPN). SmartGATE provides secure electronic commerce for virtually any TCP/IP application on the Internet through mutual authentication and session encryption and high-level database protection.	According to the Product Cost List provided, Gauntlet PC Extenders for both Windows 3.1 and Win95 are $100 each. All SmartGATE servers are $6000, and the Gauntlet Internet Firewall systems can cost as high as $17,000.
UNISYS	SERVICE Unisys CoolICE (Internet Commerce Enabler), is a software integration solution that allows management of a mixture of static and dynamic Internet Web services via a corporate Intranet or the public Internet.	CoolICE can manage Internet documents and services, build Internet business services based on existing applications and data, provide secure Web access to applications on existing servers, and develop new Web applications based on data from multiple servers and databases. Unisys reports CoolICE will integrate with industry standard payment techniques	No specific costs provided.

Analyzing Security and Authentication Needs

Before agencies can choose among the various vendor offerings, a more basic analysis of security and authentication needs for individual projects must be undertaken. Basic judgements about security and authentication must be made by the agency and communicated to the vendors. In determining whether a given security need exists, agencies should consider questions like: how is this process implemented today?; does it require a signature?; is there a statute or regulation that requires privacy or confidentiality or individual identification?; is this an area where there has been litigation or other disputes in the past – if so, what are the problems and how do they relate to the online system?; how much financial or other legal liability exposure is there for the agency if there is a problem with this application?.

The Security and Authentication Requirements Matrix on page 26 summarizes Task Force discussions defining categories of information security. This matrix provides a draft model for analyzing security and authentication needs on a project basis.

The left column lists specific characteristics that may be a part of a single online government application. Across the right columns are security requirements broken into three levels: Network, Document and Application. To make use of the matrix, an agency would first determine which characteristics apply to their particular application. Then, reading across the right, agencies would check off appropriate security requirements for each of the application characteristics that apply. It is important to note that application characteristics are broken out to assist agencies in targeting security solutions specifically to the part of the application where such solutions are required. Security solutions can be costly, time-consuming and resource intensive and should therefore be matched closely to actual application needs.

For any given application characteristic, there is a checklist of information security requirements that might apply. These are in three levels: network, document and application. Some security only deals with the flow or control of data as it flows over a Network (including the Internet):

- Confidentiality means preventing interception and reading of the data as it flows over the network.

- Authentication for access control means only allowing certain users access to certain areas or resources on a network.

The next level, Document Security, deals with the transactional data itself - the data that actually constitutes the filing, the bid or the contract, for example. This data may need to be kept over time, secured, authenticated and so on:

- Data privacy refers to data in which a person or entity has a continuing legal interest or right. Medical records, proprietary information and financial data would usually require this type of security.

- Receipt or acknowledgement refers to those instances where confirmation of transmission receipt is required for a given document or data set.

- Authentication for binding intent refers to data that form the basis of a contract or other document that is being assented to or “signed”.

- Data integrity refers to the need to show that the data originally sent has not been tampered with during a given period of time.

The last level, Application, involves functionality available within the application:

- Authentication of Role or Authority for Specific Actions refers to an individual user's ability to perform any given function within the application such as approving data or setting user rights.

These categories overlap to some extent, but they are presented as a basis to begin thinking about information security needs for a given application in a structured and solution-oriented manner. The following example uses Comm-PASS (the State's online procurement and solicitation system) to illustrate how an agency may be able to use the matrix.

A given electronic commerce application may require one or more of the application characteristics that are listed in the left column of the matrix. CommPASS, for example, requires #4, Account Usage, for agency updates since only authorized parties may update their own information. It requires #1, Information Access, for the publishing of publicly available information. Eventually, for bid submission, that part of the application would entail #3, Legally-binding Documents. If the system allowed bidder information requests by e-mail or web form, then that would fall under #2, Information or Service Request.

Given this set of application characteristics, the applicable security requirements are then identified. For Account Usage (#4), Transmission Confidentiality at the Network level would probably be necessary. For Information Access (#1) it is likely there would be no security requirements. For Legally-binding Documents (#3), Transmission Confidentiality would be needed at the Network level; and Data Privacy, Receipt or Acknowledgement, Authentication for Binding Intent and Data Integrity would likely be needed at the Document level. Finally, for Information or Service Request (#2), it is probable that only Receipt or Acknowledgement at the Document level would be needed.

Based on the boxes checked in the matrix, an agency would then want to match up the security requirements with an available menu of technical security offerings. Such a menu would include smart cards, biometrics, Public Key cryptography, signature dynamics and other technologies offered by vendors (see Technology Matrix above). Based on an analysis of costs, benefits and risks the choice of technical offerings can be more closely tailored to the actual application needs. Further refinement of the matrix and the development of a menu of technology solutions have been recommended as part of this report.

SECURITY AND AUTHENTICATION REQUIREMENTS MATRIX

APPLICATION CHARACTERISTICS	SECURITY REQUIREMENTS						
	Network Level		Document Level				Application Level
	Transmission Confidentiality	Authentication for Access Control	Data Privacy	Receipt or Acknowledge-ment	Authentication for binding Intent	Data Integrity	Authentication of Role or Authority for Specific Actions
1. Information Access (publicly available, Web page)							
2. Information or service request (requires response or confirmation)							
3. Legally-binding documents (bids, licenses, applications, filings, notices, etc.)							
4. Account Usage (authorized use of networked data or resources)							
5. Electronic payment transactions							

Online Government Task Force

1. Introduction
The Chief Information Officer has established the Online Government Task Force to chart the immediate future course of online government in the Commonwealth of Massachusetts. The Task Force shall report to the CIO on:

a) the Commonwealth's operational needs for online government functions;
b) the legal and policy requirements for such functions, with particular emphasis on the need for authentication, integrity, confidentiality, and non-repudiability;
c) currently available and near-term technologies performing such functions;
d) central services that could promote the growth of online government;
e) the state of current technical and legal efforts in the Commonwealth, other states, the federal government, and other countries;
f) specific technical and legal information that could support agencies that are implementing or evaluating online government functions;
g) suitable candidates for pilot projects for evaluating online government solutions.

2. Operational Needs for Online Government
The Task Force should explicitly identify the Commonwealth's range of operations that could be performed better or more efficiently using online technologies. The Task Force should identify online government projects that are being implemented now and are planned or desired in the short term by agencies. The Task Force should identify and categorize the types of government functions that are ripe for networked automation. The scope should extend to both Internet and Intranet communications.

3. Legal and Policy Requirements for Online Government
The Task Force should identify and categorize the functionality needed for online government functions to comply with business, legal, and policy requirements. Specifically, the Task Force should evaluate requirements for authenticity, integrity, confidentiality, and non-repudiability of network communications, with particular emphasis on the suitability of PKI technologies.

4. Current Technology
The Task Force should assess the current and near-term state of the technology available to meet the business, legal, and policy needs of the Commonwealth. This includes testing or demonstrating relevant technology. This effort should result in a narrative and/or a matrix that represents a thorough evaluation of current offerings by PKI and other vendors, as well as an assessment of the strengths and weaknesses of these solutions.

5. Central Services for Promoting Online Government
Given the business, legal, and policy requirements, and the technologies available to meet them, the Task Force should identify key central services, particularly PKI services, that would promote the use of online technologies by state agencies.

6. Standards and Guidance for Agencies
The Task Force should develop specific standards and guidance for agencies that wish to implement online government solutions. The emphasis should be on concrete, practical advice that can materially assist agencies that have advanced to the point of implementing an online government operation. In addition to this specific guidance, the Task Force should also develop information and advice for agencies that wish to evaluate the benefits of online technologies. This and/or other material should also serve to give agency management the information they need to appreciate and support online technologies.

7. Pilot Projects
As a result of identifying business needs, legal and policy requirements, available technologies, and the appropriate central role for the state, the Task Force should propose suitable candidates for pilot projects for evaluating online government solutions.

8. Members of the PKI Task Force
Membership in the task force is open to any public entity in the Commonwealth. Anyone interested in joining the task force or receiving more information should contact Dan Greenwood at dgreenwood@state.ma.us or 617.973.0071.

The Commonwealth of Massachusetts
Executive Office for Administration and Finance
Information Technology Division

One Ashburton Place • Room 801 • Boston • Massachusetts • 02108

ARGEO PAUL CELLUCCI
GOVERNOR
CHARLES D. BAKER
SECRETARY
T. LOUIS GUTIERREZ
CHIEF INFORMATION OFFICER

Telephone: (617)973-0762
Facsimile: (617)727-3766

August 25, 1997

TO: Cabinet Secretaries
Agency Heads
System Directors

I have convened an "Online Government Task Force" to explore and report on current and recommended uses of electronic commerce technologies and practices for the Commonwealth. I am especially interested in assisting agencies to use the Internet for state business transactions. Such initiatives may be as simple as enabling citizens to query public information at your agency over the Internet, or as bottom-line oriented as setting up secure online filings and payments. The aim is to deploy public network technologies to reduce costs and enhance service quality to citizens and businesses that interact with us.

The Task Force is paying particular attention to the legal and technical requirements for information security. It is important to the statewide planning effort that the appropriate person(s) at your agency completes the attached survey for each electronic commerce project you may have underway or planned. Because of our concern that constituents and state business partners not find themselves faced with incompatible or fragmented technologies as agencies begin to bring their business online, agency participation in this survey is essential to having executive branch agency initiatives endorsed and supported in the statewide online government plan.

The Information Technology Division will be allocating some of its MAGNet information technology investment funds in FY98 to assist selected agencies in implementing projects identified through this survey, in the form of matching funds.

Your staff may submit the attached survey, or complete the survey online at http://www.state.ma.us/itd/ogtf.htm. If you have any questions about the survey or the Task Force, please contact Dan Greenwood by telephone at (617) 973-0071 or by sending e-mail to Dan.Greenwood@state.ma.us.

Thank you very much for your assistance with this exciting and important endeavor.

Sincerely,

T. Louis Gutierrez,
Chief Information Officer

Online Government Task Force Project Survey

Agency: _____
Name of project: _____
Brief description: _____
Contact name: _____ telephone: _____ e-mail: _____

1. This project will be based on:
- ❍ an existing (or "legacy") system with few or no changes
- *or* ❍ a replacement for an existing system
- *or* ❍ a completely new system

2. Users will be accessing the system *(select all that apply)* :
- ❑ from within the state/agency network (MAGNet)
- ❑ from within a state network external to MAGNet
- ❑ from the Internet

3. Users of this system are:
- ❍ not known in advance
- *or* ❍ of a known community *(select all that apply)*:
  - ❑ state field workers
  - ❑ state regional offices
  - ❑ contracted providers
  - ❑ regulated businesses or professionals
  - ❑ Massachusetts local governments
  - ❑ other governments (federal, other states, etc.)
- *or* ❍ pre-identified through some other process- *please describe*:

_____

4. Users will be able to *(select all that apply)*:
- ❑ query (search) a database
- ❑ update a database (submit information)
- ❑ pay fees- required
- ❑ pay fees- optional
- ❑ other- *please describe*: _____

5. Verifying the identity of the user ("authentication") is:
- ❍ not required.
- *or* ❍ required, with a ❑high, ❑medium, or ❑low degree of certainty.

How is identity established in your current system?

_____

6. Will statutory or regulatory changes be needed for this project? ❑yes ❑no

7.
- ❍ Communications do not need to be secured.
- *or* ❍ Communications need to be secured:
  - ❑ to ensure privacy or confidentiality
  - ❑ for non-repudiation (proof that a particular person sent particular data)
  - ❑ for access control (authenticate users and what they can do)

8. At what stage is this project:
- ❍ being conceptualized
- *or* ❍ concept accepted, being designed or planned
- *or* ❍ funding and resources identified/committed
- *or* ❍ work is being done!

This survey can be completed online at **http://www.state.ma.us/itd/ogtf.htm**, or send paper to: Dan Greenwood, Information Technology Division, rm. 801, One Ashburton Place, Boston, MA, 02108

AGENCY PROJECT SURVEY RESULTS

Agency and Project	Legacy Based System	User Access			Functionality				Security Need				Stage
		Internet	Inside MAGNet	Users and Relationship	Query	Update	Pay Fees-Req.	Other	Authentication	Privacy	Non-Repudiation	Access Control	
Bureau of Special Investigations: Investigator's System	No	No	Yes	State field workers; state regional offices. Known internal party	Yes	Yes			Yes	Yes	No	No	Work being done
Campaign and Political Finance: OCPF Website	No	Yes	Yes	Regulated businesses or professionals; Mass. Local govt's; other govt's. Known external party	Yes				No	No	No	No	Concept
Committee For Public Counsel Services (CPC): PC BILL	No	Yes	No	Contracted providers. Known external party				Download software	Yes	No	No	Yes	Work being done
Department of Correction: Inmate Research Statistics project	No	No	Yes	State field workers; regulated businesses or professionals; Mass. Local govts.; other govts. Known internal and external parties	Yes				No	No	Yes	No	Concept
Department of Housing and Community Development: Client and Fiscal Management System (CAFMIS)- IT2	No	Yes	Yes	State field workers; state regional offices; contracted providers; LHAs; Municipalities. Known internal and external parties	Yes	Yes			Yes	Yes	Yes	Yes	Work being done
Department of Revenue: Tax Exempt/Resale Certificate Verification	No	Yes	Yes	Regulated businesses or professionals. Known external party	Yes			Validity certification	Yes	Yes	Yes	Yes	Concept
Department of Revenue: Corporate/Personal Income Tax Extensions	Yes	Yes	No	Regulated businesses or professionals. Known external party		Yes		Submit extensions	Yes	Yes	Yes	Yes	Concept
Department of Revenue: Customer Feedback Form	No	Yes	No	Regulated businesses or professionals				Submit info	No	Yes	Yes	Yes	Concept
Department of Revenue: Electronic Funds Transfer (EFT) Application	Yes	Yes	No	Regulated businesses or professionals. Known external party		Yes		Submit EFT application	Yes	Yes	Yes	Yes	Concept
Department of Revenue: Taxpayer Change of Address Form	Yes	Yes	Yes	Registered tax-payers. Known external party		Yes			Yes	Yes	Yes	Yes	Concept

Agency and Project	Legacy Based System	User Access			Functionality				Security Need				Stage
		Internet	Inside MAGNet	Users and Relationship	Query	Update	Pay Fees-Req.	Other	Authentication	Privacy	Non-Repudiation	Access Control	
Division of Banks: Authenticated Internet Forms Filing	No	Yes	No	Pilot Banks. Known external party	Yes	Yes	No		Yes	Yes	Yes	Yes	work being done
EOHHS: Client Index	No	No	Yes	Management personnel in executive office and possibly agencies. Known internal party	Yes				Yes	Yes	No	No	Work being done
Executive Office of Environmental Affairs: Internet Access to GIS	Yes	Yes	Yes	Possibly restrict use to liscensed site professionals. Known external party	Yes			Call up predefined map	No	No	No	No	Work being done
Executive Office of Public Safety: Public Safety's Non-Confidential Information	No	Yes	Yes	General public. Unknown external party	Yes				No	No	No	No	Design
Fisheries, Wildlife and Environmental Law Enforcement: SPORT	No	Yes	No	State regional offices; regulated businesses or professionals; Licensees and License Agents. Known internal and external parties	Yes	Yes	Yes	Obtain licenses, permits, registrations, etc.	No	Yes	No	Yes	Design
General Court: Massachusetts General Laws Online	No	Yes	No	General public, Public agencies. Unknown external party	No	No	No		No	No	No	No	Work being done
Holyoke Community College: Student registration over the Web	Yes	Yes	No	General public. Unknown external party			Yes	Register for classes	No	Yes	No	Yes	Design
Holyoke Community College: Student access to personal information	Yes	Yes	No	Registered students. Known external party	Yes				Yes	Yes	No	No	Work being done
Mass Highway: Incident Management	No	Yes	Yes	State field workers; state regional offices; Mass. Local gov't; emergency services. Known internal and external parties	Yes	Yes			Yes	No	Yes	Yes	Concept
Mass Highway: Federal Highway Electronic Data Exchange	No	Yes	Yes	State field workers; state regional offices; Mass. Local govt's; other govt's. Known internal and external parties	Yes	Yes		Authorize funding	Yes	No	Yes	Yes	Work being done
Mass Highway: Traffic Video Information	No	Yes	Yes	General public	Yes				No	No	No	No	Concept

Agency and Project	Legacy Based System	User Access			Functionality				Security Need				Stage
		Internet	Inside MAGNet	Users and Relationship	Query	Update	Pay Fees-Req.	Other	Authentication	Privacy	Non-Repudiation	Access Control	
Mass Highway: Graphical Information Systems Interface Map	No	Yes	Yes	State field workers; state regional offices; other govt's. Known internal and external parties	Yes			Download state maps	No	No	No	No	Concept
Massachusetts Aeronautics Commission (MAC): Airport Information Management System (AIMS)	No	Yes	Yes	State field workers; regulated businesses or professionals; Mass. Local govts.; other govts.; Airport managers, etc.; general public. Known internal and external parties and unknown external parties	Yes	Yes			Yes	Yes	Yes	Yes	Design
Mount Wachusett Community College: Distance Learning	No	Yes	No	Students and faculty. Known internal party	Yes				Yes	Yes	No	Yes	Design
North Shore Community College: EDE	No	No	No	State regional offices. Known internal party	Yes	Yes		Interface with database	Yes	No	No	Yes	Work being done
North Shore Community College: State SQL server for spending plan	Yes	No	No	Spending plan users. Known internal party	Yes	Yes			Yes	Yes	No	No	Work being done
North Shore Community College: Banner Web for Student	Yes	Yes	No	Students with ID. Known internal party	Yes	Yes	Yes		Yes	Yes	Yes	Yes	Design
Office of the Comptroller: MMARSWeb/ManagerMMars	Yes	No	Yes	Department managers. Known internal party	Yes	No	No	Pre-designed queries and reports	No	No	No	Yes	Concept
Office of the Comptroller: MMARSWeb/VendorWeb	Yes	Yes	No	Commonwealth vendors. Known external party	Yes	Yes	No		Yes	Yes	Yes	Yes	Concept
Office of the Comptroller: MARSWeb/WEBWarehouse	Yes	Yes	Yes	State employees, vendors, citizens, press. Unknown external party	Yes	No	No	7 x 24 availability	No	No	No	No	Concept
Operational Services Division: Procurement Desktop	No	No	Yes	Department staff; vendors. Known internal and external parties	Yes	Yes	Yes	Order and payment process; updates MMARS	Yes	Yes	Yes	Yes	Concept

Agency and Project	Legacy Based System	User Access			Functionality				Security Need				Stage
		Internet	Inside MAGNet	Users and Relationship	Query	Update	Pay Fees-Req.	Other	Authentication	Privacy	Non-Repudiation	Access Control	
Operational Services Division: Comm-Pass	No	Yes	Yes	All Prospective Bidders; public agencies, general public. Unknown external party	Yes	Yes	No		Yes	No	No	Yes	Work being done
Registry of Motor Vehicles: Express Lane	Yes	Yes	No	General public. Unknown external party	No	Yes	Yes	Issues a confirmation of your order.	Yes	Yes	No	No	Work being done
Secretary of State: Voter Information	Yes	Yes	No	General public. Unknown external party	Yes				No	No	No	No	Concept
Worcester State College: Colleague INTERNET Access	Yes	Yes	No	General public. Unknown external party	Yes	Yes			No	No	No	No	Design

Request for Information
Secure Online Transactions

Thursday, April 24, 1997

The Commonwealth of Massachusetts, acting through the online Government Task Force, is contemplating the release of one or more procurements for electronic commerce products and/or services. This Request for Information (RFI) is intended to solicit information that could be useful in drafting subsequent RFRs. This RFI specifically seeks information on products and/or services that will enable the Commonwealth of Massachusetts to use the Internet and internal networks for secure messaging and transactions.

Section 1: Background

The Chief Information Officer for the Commonwealth of Massachusetts has convened the Online Government Task Force to chart the immediate future course of online government in Massachusetts. The Task Force consists of representatives from a number of different agencies, departments and offices of the Commonwealth. The Task Force is investigating solutions that improve efficiency and service quality using internal and Internet-based electronic communications that possess authentication (to achieve access control as well as non-repudiation), integrity, and confidentiality.

The Commonwealth has made information technology (IT) development and electronic communications a priority, spending approximately $350 million on IT annually. The Commonwealth seeks to make a large number of routine business transactions available over the Internet and internal networks, with the intent that they will be performed for less cost and conducted at a higher quality service level for citizens, regulated entities, vendors and others. The Commonwealth seeks to create methods for secure access to a number of business transactions via electronic media, including licensing, permitting, applications, filings, procurement and a host of other functions. Internally, the Intranet is being looked at as a potential mechanism to alleviate the crush of paper associated with a large number of routine state government functions, including personnel, procurement drafting, and other collaborative data sharing, work flow or messaging applications.

Today, the Registry of Motor Vehicles (RMV) processes a number of transactions and accepts credit card payment over the state web site. The RMV transactions assure the confidentiality of credit card data over the Internet by use of public key cryptography implemented with the SSL 2 protocol. The Division of Banks (DOB) has embarked on a pilot project to receive authenticated online filings by banks over the state web site. The DOB pilot assures the data is confidential and the identity of

the filing bank and individual filer is authenticated by use of public key cryptography implemented with the SSL 3 protocol. The banks participating in the DOB pilot are issued standard X.509v3 digital certificates associated with the bank public key.

While the Task Force is interested in all relevant replies to this request for information, responses that propose cost effective and currently available methods to assure non-repudiation are of particular interest. Non-repudiation means a method to prevent or sufficiently rebut subsequent denial of transmittal or receipt of a given message or participation in a given transaction. In some cases, this non-repudiation must be capable of tying an individual to a particular piece or set of data at a particular time. For non-repudiation, mere access control based on an SSL 3 implementation of public key cryptography and digital certificates will not suffice, unless some additional technique exists to bind the identity of a given party to the message or transaction engaged in by that party.

Section 2: Purpose of RFI

The Task Force seeks responses from vendors which offer information about currently- available solutions to any or all of the following business needs and example applications:

2.1 Internet access with Authentication.

Such an application would involve access via the Internet to Commonwealth data located behind the firewall.

Example:

Certain companies, for a legitimate business purpose, need to know the driving records of certain employees. A solution is needed that will allow a pre-selected group of companies to access employee driver histories and determine driver status from a state database. Access control is required to allow companies to access only the driving records of their employees.

General Considerations:

Authentication, in the example above, is being utilized to assure access control to defined data on the network. Assuming the data is being viewed with a web browser, then some provision may also be required to assure the data remains confidential and has not been altered while in transit over the Internet.

2.2 Internet-based data submission with non-persistent connection.

Such an application would involve access via the Internet to a Commonwealth database behind the firewall for the purpose of submitting information.

Example 1:

For the purpose of posting requests for response as part of a procurement, certain users would be allowed access to a state procurement services database, provided authentication and non-repudiation is available for each submission.

Example 2:

For the purpose of applying for a professional or commercial license renewal, certain users would be allowed access to a state license database, where the application form would be electronically delivered. As in the previous example, non-repudiation is required to prevent the applicant from denying information submitted in the application and to provide proof that the state received a particular application.

General Considerations:

The posting of bids in response to a procurement and the submission of a license application raise a number of issues that are unique to those processes. The Commonwealth will be performing a number of other transactions as well, including grant applications, online permitting and various filings with state agencies. The Commonwealth will pursue some transactions under this category (Internet-based data submission with non-persistent connection) that will not require non-repudiation. Some of these transactions would require only front-end authentication for access control, other transactions would not require authentication of the identity of the person submitting data for either access control or non-repudiation. However, the Task Force is particularly interested in information relating to non-repudiation.

2.3 Internet-based data exchange with persistent connection.

Such an application would involve access via the Internet to an online application located behind the firewall such that the user would be authenticated once, and the system would maintain the identity of the user in all portions of the application throughout the duration of the session.

Example:

For the purpose of negotiating and crafting contract agreements, both state users and non-governmental users would be allowed access to a common document management and electronic workflow application, with all users considered "members" of the workflow and able to perform tasks in the workflow. The application front-end allows users to submit documents, edit documents and query databases behind the firewall.

Section 3: Environment

The following diagram describes the Commonwealth's current and near-term computing and communications environment. See Attachment 1.

Section 4: Other Considerations

Interested vendors may provide information regarding products, services and/or integrated solutions that address either some or all of the above-mentioned business needs. The purpose of this RFI is to provide the Commonwealth with information that could be useful in developing one or more RFRs for secure online transactions and messaging. Please feel free to respond to any specific questions in this RFI or to

offer any other information that you feel could be useful to the Commonwealth in making decisions about an RFR. In addition to the questions raised in the previous sections, the Commonwealth is interested in information on the following.

4.1 Identify and describe all software or hardware required on a client workstation for the proposed product/service/solution.

4.2 Identify and describe any back-end software or hardware required of the proposed product/service/solution.

4.3 Describe how your product/service/solution scales to the enterprise.

4.4 What are the short, mid and long term electronic records archival ramifications of the proposed product/service/solution, including suitability for audit and admissibility in evidence in a court?

4.5 How is the product/service/solution compliant with the provisions of the Americans with Disabilities Act?

4.6 How is the product/service/solution Year 2000 compliant?

4.7 What, if any, privacy concerns are raised by the authentication techniques proposed and how are those concerns addressed?

4.8 Does the proposed product/service/solution offer any online payment capabilities? Please describe.

4.9 Describe any current implementations of your product/service/solution and note any business partners involved with that implementation.

4.10 Provide information about your company and its history.

4.11 Provide cost information about the proposed product/service/solution.

Section 5: Procedural Information

This RFI is not an offer or solicitation and does not obligate or bind the Commonwealth to procure any goods or services as a consequence. Responses to this RFI do not constitute bids or proposals and are not legally binding on the responding party. Respondents may not charge ITD or the Commonwealth of Massachusetts for any costs associated with the preparation of responses to this RFI. This RFI is being released on Commonwealth's Procurement Access and Solicitation System (Comm-PASS). A copy of this RFI is also available at ITD's legal department web site at <http://www.state.ma.us/itd/legal>. The schedule of events for this RFI, subject to amendment, is:

Thursday, April 24, 1997	RFI released on Comm-PASS
Friday, May 2, 1997	Informational session
Monday, May 12, 1997	Responses due

The informational session will be held at One Ashburton Place, Room 801, Boston, MA 02108 from 10:00 am to 11:00 am. Please inform the chairman of the procurement management team (preferably by e-mail) if you will attend the session so that adequate seating can be made available. Organizations or individuals responding to this RFI should submit ten copies of their response in writing, accompanied by any attachments, exhibits or software, to the chairman of the procurement management team by 5:00 pm on Monday, May 12, 1997. Responses must also be submitted via e-mail or on floppy disk in Word for Windows, WordPerfect format, or as a Text-Only document. The chairman of the procurement management team is:

Dan Greenwood, Deputy General Counsel, Information Technology Division
Online Government Task Force, Team Leader
One Ashburton Place, Room 801
Boston, MA 02108
617.973.0071
<dgreenwood@state.ma.us>

Appendix D: Electronic Authentication Primer

PKI and Other Authentication Technology

There are many ways to create an electronic signature. These can range from simple methods, such as typing a name at the bottom of an e-mail message, to more complex and secure methods involving biometric technologies, such as fingerprint or retinal scans. Other types of authentication methods that are used to create electronic signatures include the use of magnetic stripe cards and PIN numbers, user names and passwords, public key cryptography, writing tablets with electronic pens, or even smart cards that generate a unique access code every few seconds. As technology advances, the list of viable alternatives is certain to grow.

Because there are so many ways to create an electronic signature, and because many of them do not resemble a holographic "autograph," many law reform efforts have adopted the term "authentication" rather than "signature." For example, the current drafts of Uniform Commercial Code Articles 2 and 2B eliminate the term "sign" and instead allow the authenticity of documents to be proven in any reasonable manner.[1] These drafts also clarify that assent may be manifested through any form of authentication, including proof of the authentication process itself.[2]

One of the most interesting and robust technologies being used and developed for authentication purposes is known as public key cryptography, which allows for a very high degree of reliability when implemented properly. A "digital signature" does not refer to the image of a signature in any way. Unlike an "electronic signature" which is simply any symbol or process intended to be a signature and a "digitized signature" which refers to an electronic image of a signature, a "digital signature" is actually a term of art that refers to the scrambling of data in order to provide security and authentication. While the technical details of public key cryptography are extremely complex and have limited utility to a broader audience, an understanding of the basic concepts is both accessible and useful. Due to the current interest in deploying large-scale public key systems, it is likely that this technology will touch many areas of the economy. In fact, the growth of public key systems in many sectors of the economy suggests that a rudimentary knowledge of these concepts will serve lawyers well when legal questions arise as a result of this technology.

The Basics of Public Key Cryptography

Codes and cryptography are thousands of years old. Although cryptography became much more sophisticated in modern times, it still relied on both the sender and the receiver knowing the same "secret key" to encode and then decode messages. To be secure, a secret key coding

---

[1] According to the UCC March 21, 1997 Draft 2B-102(a)(2) and the UCC May 16, 1997 Draft 2-102(a)(1) "'Authenticate' means to sign or to execute or adopt a symbol, including a digital signal and identifier, or to do an act that to encrypt a record or an electronic message in whole or in part, with present intent to adopt, establish the authenticity of, or signify a party's acceptance and adoption of, a record or term that contains the authentication or to which a record containing the authentication refers." Under Reporter's Note 2 of the same section it is explained that "This article replaces the traditional idea of "signature" or "signed " with a term that incorporates modern electronic systems, including all forms of encryption or digital symbol systems. Substantive rules on proof of authentication are in Section 2B-[114]. Basically, the fact of authentication can be proved in any manner including proof of a process that necessarily resulted in authentication. Use of an "attribution procedure" agreed to by the parties per se establishes that a symbol or act constitutes an authentication."

[2] See UCC March 21, 1997 Draft 2B-112, 2B-114(b): "A record or message is authenticated as a matter of law if the symbol executed or adopted by a party complies with an attribution procedure for authentication agreed to or adopted by the parties. Otherwise, authentication may be proven in any manner, including by showing that a procedure existed by which a party necessarily must have executed or adopted a symbol in order to proceed further in the use or processing of the information."

system requires some method for distributing the secret key to intended users without it falling into the hands of other parties.

The basic nature of the Internet makes it poorly suited for a secret key system because it is an "open" network in which messages may make several "stops" before arriving at their final destination. This creates a serious risk that a third party could intercept a secret key at some point along its routing, which would allow him to read encoded messages or even send coded messages purporting to be from an authorized holder of the secret key. Physically delivering a secret key to every user by secure channels would be slow, expensive, unwieldy, and would effectively rule out serendipitous or one-time transactions between people and firms that have not previously exchanged secret keys.

Public key cryptography eliminates the need for users to share a secret key, which makes it ideally suited for communications over "open" networks such as the Internet. While the following illustration describes a complex process, the hardware and software that implements this technology will shield the end user from these details; end users will find no need to concern themselves with the complicated background operations that make the system possible.

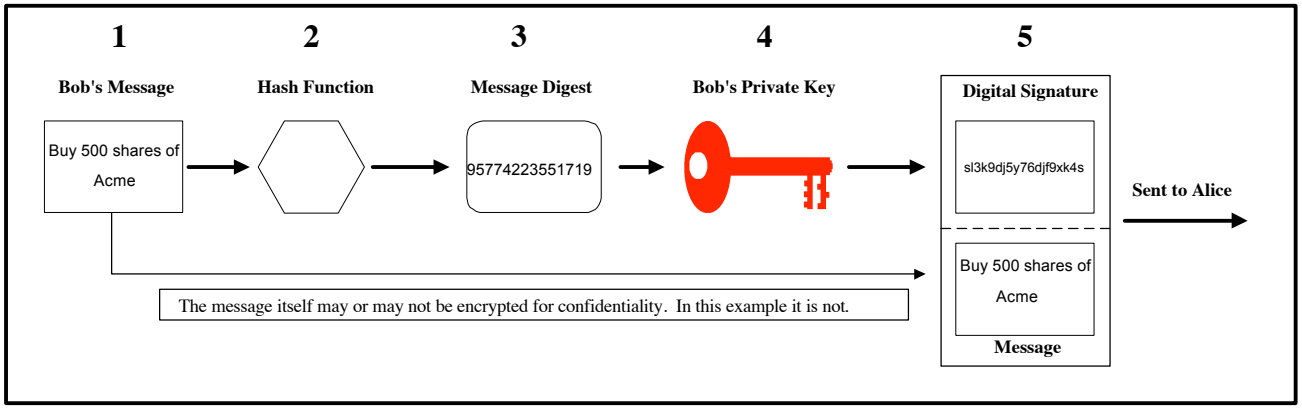
With a public key system, each user will have software that will generate two related keys known as the public key and the private key. The fundamental characteristic of these key pairs is that the public key, and only that public key, can decrypt a message encrypted with its corresponding private key. Similarly, the private key, and only that private key, can decrypt a message encrypted with its corresponding public key. As such, these key pairs are analogous to secret decoder rings from a box of cereal, where each ring fits into its companion ring and no other.[3]

Once Bob, a user, has generated his public/private key pair with a computer, he keeps his private key very secure (protected by a password on his computer or, preferably, a smart card locked in a safe) but he makes his public key freely available by sending it to people or by posting it to a public key directory on the Internet. Then, if Alice, another user, wants to send Bob a private message she can obtain Bob's public key and use it to encrypt the message. Since only Bob's private key can decrypt a message that has been encrypted with his public key, both Alice and Bob can be sure that only Bob can read the message. Thus, public key cryptography allows two people to send secure messages without the need to exchange a secret key through a secure channel. Only Bob's public key needs to be shared in order for Bob to receive completely secure messages.

This unique characteristic of public key cryptography also forms the basis for secure digital signatures. This process is illustrated in the diagram below. In order to generate a digital signature, Bob must first have a message (1) that he wants to sign and send to Alice. The message could be as simple as an e-mail message or as complicated as a lengthy contract. Bob would then run his communication to Alice through one of several standard algorithms known as hash functions (2) that performs a series of mathematical operations on the original message. The hash function produces a number called a message digest (3), which can be thought of as a fingerprint of the message, because any change in the message, no matter how slight, will cause the hash function to produce a completely different message digest. Bob then encrypts the message digest with his private key (4). The message digest encrypted with

[3] The math underlying public key cryptography is rather esoteric and is beyond the scope of this paper. In short, public key cryptography is based on the fact that the only way to factor a large prime product (a very large number derived by multiplying two large prime numbers) is by having a computer calculate every possible combination of numbers in order to find the two component numbers. If the component numbers are large enough, solving the equation becomes "computationally intractable." The current generation of public key cryptosystems uses numbers so large that it would take extremely powerful computers years, and millions of dollars, to crack a single public/private key pair.

Bob's private key forms the actual digital signature for the message.[4] Finally, Bob transmits both the digital signature and his original message to Alice (5). If Bob also wants to keep his message to Alice confidential, he could encrypt the message using Alice's public key (not shown).

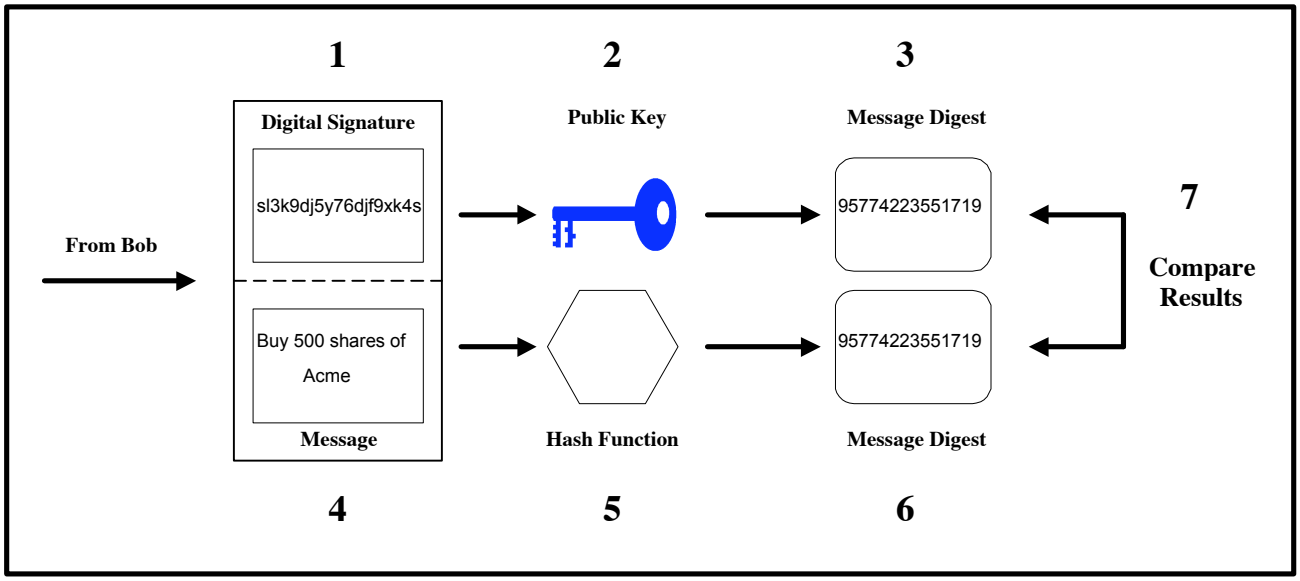


Upon receipt, Alice's computer and software would perform two separate operations to verify Bob's identity and to determine if the message had been altered in transit. As a practical matter it is not important which operation is performed first.[5] To verify Bob's identity, Alice's system would take Bob's digital signature (1) and then use Bob's public key (2) to decrypt the digital signature, which will produce the message digest (3). If this operation is successful, Alice knows for a fact that Bob, who alone has access to his private key, must have sent the message.

In order to ensure that Bob's message had not been altered in transit, Alice would run Bob's message (4) through the same hash function (5) that Bob used, which would yield a message digest of Bob's message (6). Alice would then compare the two-message digests (7), and if they were the same she would know for a fact that the message had not been altered in transit.

[4] The digital signature is created through two distinct steps: First, the message digest, created through the use of a hash function, ensures the integrity of the content of the intended communication. Second, the use of the private key to encrypt the message digest authenticates the identity of the person sending the message.

[5] The two operations are performed upon separate documents. One upon the digital signature, an encrypted message digest, and the other upon the message itself. Although the results of both operations are compared against each other to obtain a true verification, it is irrelevant which operation is performed first.



Thus, public key cryptography allows people and businesses to exchange messages over open networks with a high degree of confidence that those messages are confidential (unable to be read by unauthorized persons), authentic (sender's identity can be verified), and accurate (the message can not be altered without detection). This is a level of security far greater than that afforded by ink signatures. This technology can enable the use of online systems to send and receive tax returns, purchase orders, mortgage applications, credit card orders, and any other type of sensitive or official information with greater security than if the transactions were conducted on paper.

However, nothing said so far would rule out the possibility that an impostor could generate a public/private key pair and then post the public key on the Internet claiming it belongs to Bob. Unaware of the deception, Alice might then use this public key to send messages that the impostor, but not Bob, could read. The impostor could also use the fake private key to digitally sign messages that Alice would assume Bob sent because they can be decoded using the public key which Alice does not yet realize is fraudulent. In order to prevent this, parties relying on digital signatures must have confidence that the public key on the Internet that purports to belong to Bob is, in fact, owned by him. This function is performed by a trusted third party known as a certification authority (CA), which binds the identity of a particular party to a particular public key and, by implication, a particular private key.

CAs do this by issuing a digital certificate. A digital certificate is a small electronic record that (i) identifies the CA issuing it, (ii) identifies the subscriber, (iii) contains the subscriber's public key, and (iv) is digitally signed with the CA's private key. The digital certificate can also contain additional information, including a reliance limit or a reference to the CA's "certification practice statement" that gives relying parties notice of the level of inquiry conducted by the CA before issuing the certificate.

To obtain a digital certificate, Bob would present the CA with a copy of his public key along with sufficient proof of his identity. For digital certificates that could be used for larger transactions, the CA might charge a higher fee and require greater proof of identity. Once satisfied as to the identity of the subscriber, the CA would issue the subscriber a digital certificate. When Bob wants to use his digital signature, he would also transmit a copy of his digital certificate to Alice. In addition to the steps described above, upon receipt of Bob's message Alice's computer would also confirm with the CA identified in the digital certificate that Bob is who he purports to be and that his certificate has not expired or been revoked. If

Bob learns or fears that his private key has been compromised, he would notify his CA of this fact so that it could post that information to its "certificate revocation list." All of this activity would take place in the background, unseen and unnoticed by Alice, and would happen in much the same way as it occurs with online credit card validation systems.

One of the major unanswered questions about the use of public key cryptography for digital signatures, and a major point of contention between advocates of different types of electronic signature laws, relates to the business model for CA services that will ultimately prevail in the marketplace. A Public Key Infrastructure (PKI) will need to evolve to support use of this technology[6]. While advances in technology will certainly create new possibilities not presently contemplated, the two primary business models currently vying for support are known as the "open PKI" and "closed PKI" models.

An open PKI model assumes that subscribers will obtain a digital certificate from a CA that will securely link their identity to their public key for all, or at least many, purposes. Thus, in an open PKI environment a person could obtain a digital certificate and then use it to order goods online from various merchants, sign legally binding agreements, or even file documents with a government entity. Subscribers could use their certificate for any transaction requiring a digital signature. In the closed PKI model, users would obtain a different digital certificate for each community of interests with which they interact online. For example, a user could have one certificate for transactions with their bank, a different certificate for communications with their employer, and yet another certificate for dealings with their health care provider.

The difference between the two models is significant. Under an open PKI model, a person's certificate could potentially be used to sign any document, which makes the consequences extremely severe if the user's private key is compromised. In a closed PKI, on the other hand, the risks to the user and the CA from an improperly signed document are more limited due to the system's more narrowly defined scope. Furthermore, the members of a particular community within a closed PKI system may enter into agreements that define the rights and responsibilities of the members, which would further reduce the risks and uncertainty in such a system.

Emerging PKI Standards

Secure Electronic Transactions (SET) is an online payment standard for credit cards. It involves the use of X.509 certificates. This standard is not widely used at this time. Other payment methods include the Cybercash method, E-Check and Millicent.

The Secure Multipurpose Internet Mail Extensions (S/MIME) standard allows e-mail to be digitally signed and sent with an associated public key certificate. S/MIME not comes standard with Netscape Communicator. Secure Sockets Layer (SSL) comes in two varieties: version 2 and version 3. Version 2 enables point to point encryption between a browser and a server. This accomplishes message confidentiality while the data is in transit over the Internet. Version 3 also allows for the exchange of certificates between the browser and server and permits authentication based on the information contained in those certificates. SSL2 is widely used and SSL3 is becoming more popular. Secure Hyper Text Transfer Protocol (S/HTTP) is an http level hashed, secured and sent with the respective public key certificate. This allows for any data that flows between a browser and a web server to be authenticated and confidential. There are many other relevant standards, but these are the ones the Commonwealth has dealt with more frequently.

[6] The acronym PKI stands for Public Key Infrastructure, reflecting the fact that the use of digital signatures based on public key cryptography requires an elaborate infrastructure (technical, business, policy, and legal) to support their use.

Non-PKI Technology: The Importance of Maintaining Options

As mentioned earlier, a number of other technologies exist to achieve electronic authentication. One very important technology is known as Signature Dynamics. It is a mechanism for the secure capture, management and verification of handwritten signatures by electronic means.

PenOp was the only company to reply to the Task Force Request for Information to the vendor community that implements Signature Dynamics. PenOp captures signatures simply and reliably, and enables them to be securely stored and safely transported between different systems. For evidential purposes, PenOp signatures can verify the authenticity of the transaction on which they were signed; PenOp can also verify the authenticity of the signature on the document with an accuracy and speed unparalleled in the paper domain. In so doing, PenOp satisfies regulatory and legal requirements for handwritten signatures.

For the signatory, PenOp's major attraction is the familiarity of submitting their normal handwritten signature - using a pen. For corporate users, the main benefit is that they can complete business processes electronically, achieving major cost savings by reducing the need for paper. It is also worth noting that PenOp removes the need for passwords and PINs, public/private key pairs or certificates.

The California Digital Signature Regulations address Signature Dynamics as follows:

California Administrative Code Title 2. CHAPTER 10.

Section 22003(b) List of Acceptable Technologies

The technology known as "Signature Dynamics" is an acceptable technology for use by public entities in California, provided that the signature is created consistent with the provisions in Section 22003(b)(1)-(5).

1.Definitions – For the purposes of Section 22003(b), and unless the context expressly indicates otherwise:

A."Handwriting Measurements" means the metrics of the shapes, speeds and/or other distinguishing features of a signature as the person writes it by hand with a pen or stylus on a flat surface.

B."Signature Digest" is the resulting bit-string produced when a signature is tied to a document using Signature Dynamics.

C."Expert" means a person with demonstrable skill and knowledge based on training and experience who would qualify as an expert pursuant to California Evidence Code §720.

D."Signature Dynamics" means measuring the way a person writes his or her signature by hand on a flat surface and binding the measurements to a message through the use of cryptographic techniques.

2.California Government Code §16.5 requires that a digital signature be 'unique to the person using it.' A signature digest produced by Signature Dynamics technology may be considered unique to the person using it, if:

A.The signature digest records the handwriting measurements of the person signing the document using signature dynamics technology, and

B.the signature digest is cryptographically bound to the handwriting measurements, and

C.after the signature digest has been bound to the handwriting measurements, it is computationally infeasible to separate the handwriting measurements and bind them to a different signature digest.

3.California Government Code §16.5 requires that a digital signature be capable of verification. A signature digest produced by signature dynamics technology is capable of verification if:

A.the acceptor of the digitally signed message obtains the handwriting measurements for purposes of comparison, and

B.if signature verification is a required component of a transaction with a public entity, the handwriting measurements can allow an expert handwriting and document examiner to assess the authenticity of a signature.

4.California Government Code §16.5 requires that a digital signature remain 'under the sole control of the person using it'. A signature digest is under the sole control of the person using it if:

A.the signature digest captures the handwriting measurements and cryptographically binds them to the message directed by the signer and to no other message, and

B.the signature digest makes it computationally infeasible for the handwriting measurements to be bound to any other message.

5.The signature digest produced by signature dynamics technology must be linked to the message in such a way that if the data in the message are changed, the signature digest is invalidated.

Appendix E: ADA and Privacy Policy Discussions

Americans with Disabilities Act (ADA)

State Agency Web sites MUST be accessible to users with non-graphical browsers. The following excerpts are from a U.S. Department of Justice technical assistance letter. The full letter can be found at http://www.usdoj.gov/crt/foia/tal712.txt.

- "The Americans with Disabilities Act (ADA) requires State and local governments and places of public accommodation to furnish appropriate auxiliary aids and services where necessary to ensure effective communication with individuals with disabilities."

- "Covered entities that use the Internet for communications regarding their programs, goods, or services must be prepared to offer those communications through accessible means as well."

- "Instead of providing full accessibility through the Internet directly, covered entities may also offer other alternate accessible formats, such as Braille, large print, and/or audio materials, to communicate the information contained in web pages to people with visual impairments. The availability of such materials should be noted in a text (i.e., screen-readable) format on the web page, along with instructions for obtaining the materials, so that people with disabilities using the Internet will know how to obtain the accessible formats."

In brief, there are three major areas that may cause an agency web site to be non-compliant:

1. Web sites that use frames that do not have fully equivalent access methods for browsers that do not support frames. (Text-based browsers cannot support frames, which are based on the concept of having different windows.)

2. Web sites that post information in PDF format without providing online access to text equivalents or detailed information on how to obtain Braille or audio versions. Adobe has set up a service (http://access.adobe.com/) that converts PDF to HTML either on the fly or as an e-mail service. Unfortunately, it has been frequently unavailable during normal business hours in the past few weeks. If this is a temporary phenomenon, including information on using this service may meet a Department's ADA compliance requirements.

3. Use of images without specifying alternate text or, in the case of image maps, alternate navigation methods.

Sarah Bourne, Task Force Member and Director of the Commonwealth's Internet Services Group, has put together a web page with links to web sites that can help agencies test their pages for compliance. Information on designing for accessibility and general information on the Americans with Disabilities Act is also available at this site. The page can be found at http://www.state.ma.us/webmass/ada.htm.

Privacy

There is an inherent tension between the individual's right to privacy and the government's need for personal information, the dimensions of which conflict have evolved over time in response to changes in technology and government's role in society. The relatively recent deployment of sophisticated information technology tools in the service of the pervasive modern state has raised a host of unique variations on this historic theme. The following

discussion seeks to provide context for thinking about the privacy issues that confront the Commonwealth, a description and assessment of our current policies, and some suggestions for improvements.

Context

Massachusetts state government is a massive service delivery organization with huge information and transaction processing operations. In conducting these operations, the state gathers, uses, and disseminates vast amounts of information, much of which relates to specific, identifiable individuals. The widespread use of information technology means that this information can be permanently stored, rapidly analyzed and extracted, cross matched with other digital records, copied perfectly an unlimited number of times, and transmitted almost instantly. This digital revolution has caused a qualitative change in the nature and character of government records, as well as a quantitative change in the amounts of information the government collects and stores.

Starting in the early 1970s, first the federal government and then the states responded to the introduction of mainframe information systems by enacted privacy statutes that attempted to strike an appropriate balance between government's need for information, the importance of open public access to government information, and the protection of personal privacy. Since then, the PC revolution that started in the early 1980s, and the networking revolution of the 1990s, have significantly altered the technical base upon which this balance was struck. These new technologies make it increasingly possible to construct virtual dossiers on people composed of information about their every interaction with any government agency. Even innocuous personal information can become a constituent piece in a much more invasive compilation of data. The impact of these changes on what is ultimately a core libertarian value requires a fresh assessment of the government's privacy policies.

One of the problems for policy makers in coming to grips with privacy issues is that the subject seems to crop up in an incredible variety of contexts. Part of this confusion can be eliminated by realizing that "the right to privacy," as it is currently understood, has three fairly distinct branches:

- **Search and Seizure Privacy.** The oldest and most explicit right to privacy is the constitutional right to be free from unreasonable searches and seizures. This provision applies only to government action and generally only in criminal or regulatory matters. Search and seizure privacy arises in the context of house searches, electronic surveillance, drug tests, drunk driving roadblocks, and the like.

- **Decisional Privacy.** First articulated by the Supreme Court in the 1960s and 1970s, and subsequently found in the Massachusetts constitution by the SJC, this is the constitutional right to be free from unwarranted government interference when making certain fundamental personal decisions. Decisional privacy arises primarily in contraception, abortion, "right to die," and sexual orientation cases.

- **Informational Privacy.** Originally a common law tort doctrine, until privacy statutes came along in the 1970s, informational privacy concerns the individual's right to control, or at least influence, the terms under which personal information is shared with others. The cluster of rights falling under the heading of informational privacy all flow from the belief that the inherent dignity and worth of individuals dictates that they have a central say in how they choose to present information about themselves to the world.

Information technology has had an impact on each of these three areas. Ultimately, however, its greatest impact is in on informational privacy, and it is this particular dimension of "the right to privacy" that is the focus of this memo. Government's policies on informational privacy affect not only taxpayers, beneficiaries, and customers (broadly speaking), but also its vendors and employees. In addition to rules for its own information, the government can choose to, or refuse to, regulate the information practices of private sector entities (both profit and nonprofit).

In evaluating the Commonwealth's performance in this regard, it is worth remembering three things. First, concerns about informational privacy are widespread, with recent surveys showing that 80% of people are concerned about threats to personal privacy, and that a majority believes existing laws are inadequate and need to be tightened. Second, privacy is a subjective concept: 25% of the population favors sharp restrictions on the use of personal information, another 18% are mostly unconcerned with privacy issues, and 57% are privacy pragmatists that care about privacy but acknowledge the need to supply personal information in exchange for other values.

Finally, information is the lifeblood of state government's operations and is indispensable in implementing the policy choices of elected leaders. As such, restrictions on the government's information practices (and this is equally true of restrictions on private sector practices) should be subject to a cost/benefit analysis. For example, you can't provide human service benefits effectively, or detect fraud, without gathering a great deal of personal information. Nor can you tax, regulate, or perform a host of other government services without such information. And you can't have an open, accountable government without allowing broad public access to government information. So, it is important to bear in mind that the resolution of most of the issues presented here requires striking the correct balance rather than picking the right side.

The Current Situation in Massachusetts: Government Information Practices

The principal laws governing the government's collection, use, and dissemination of personal information are the Public Records Law (PRL) the Fair Information Practices Act (FIPA), and a host of restrictions bound throughout the General Laws. Massachusetts also has a privacy statute (M.G.L. c. 214, s. 1B), enacted in 1974, which provides: "A person shall have a right against unreasonable, substantial or serious interference with his privacy." The SJC has said this statute codifies the common law privacy torts, but it is of little relevance for government records because the SJC has ruled that it affords less privacy protection than the non-disclosure provisions of the PRL. While somewhat convoluted and obscure, this combination of laws establishes restrictions on the use of personal information that are more robust than those of many, perhaps most, states. Improvements can and should be made, but it is not true that Massachusetts lacks a statutory framework for protecting informational privacy.

The starting point for considering informational privacy is the PRL, which divides all government information into public and non-public records. In general, all government records, including computer files, are available for public inspection or copying unless they fall within one or more of twelve exemptions. The first exemption is for records "specifically or by necessary implication exempted from disclosure by statute." I am unaware of any comprehensive compilation of these restrictions, but I am presently working my way through a list of over 200 sections of the General Laws that contain the words "confidential" or "confidentiality" and over 50 sections that contain the word "privacy."

Next, the PRL exempts several specific types of records: internal personnel rules and practices, policy memoranda, notebooks, investigatory records, trade secrets, pre-selection procurement documents, real property appraisals, information on licensed gun owners, test questions and answers, and health care contracts between public entities and HMOs. In addition to these specific restrictions, the PRL exempts "personnel and medical files or

information; also any other materials or data relating to a specifically named individual, the disclosure of which may constitute an unwarranted invasion of personal privacy." This exemption is patterned after a similar, though more narrowly worded exemption in the federal Freedom of Information Act that applies to information "which *would* constitute a *clearly* unwarranted invasion of personal privacy."

The meaning and interpretation of the PRL's personal privacy exemption is critical because, as will be seen below, there are no restrictions on the government's collection, use, and dissemination of personal information that is deemed to be public. In general, the SJC and the Supervisor of Public Records have taken a narrow view of the privacy exemption, ruling that it only applies to "intimate details of a highly personal nature." The SJC has shown little inclination to view more mundane types of personal information as falling within the exemption even though the U.S. Supreme Court, in interpreting the seemingly more narrow federal exemption, has found it far more favorable towards privacy rights.

In particular, the court has ruled that even if a record is merely a compilation of public facts (such as a rap sheet) that "does not mean that an individual has no interest in limiting disclosure or dissemination of the information." In addition, in upholding an agency's refusal to provide a list of its employee's home addresses to their union, the court ruled that "the only relevant public interest in disclosure to be weighed in this balance is the extent to which disclosure would serve the core purpose of the FOIA, which is contributing significantly to public understanding of the operations or activities of the government. That purpose, however, is not fostered by disclosure of information about private citizens that is accumulated in various governmental files but that reveals little or nothing about an agency's own conduct."

There are no restrictions on the government's collection, use, and dissemination of personal information that does not fall within one of the PRL's exemptions. The law containing such restrictions is the FIPA, enacted in 1975, which expressly excludes from its coverage any personal data contained in a public record. For non-public personal data the FIPA requires agencies holding such data to: identify a person responsible for FIPA compliance; inform its employees of the FIPA's requirements; not allow access to personal data unless authorized by statute or regulations or unless approved by the data subject; maintain a complete record of every access to and every use of personal data; make available to a data subject a list of the uses made of the personal data; make personal data available to a data subject; establish procedures for data subjects to contest the accuracy of their data; and not collect or maintain more personal data than is needed.