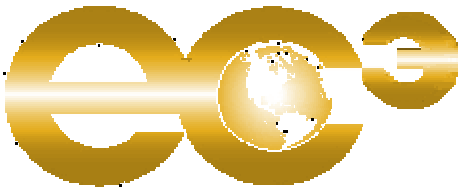
CITIZEN EXPECTATIONS FOR TRUSTWORTHY ELECTRONIC GOVERNMENT:

AN ASSESSMENT AND FRAMEWORK FOR STATE POLICY MAKERS AND INFORMATION TECHNOLOGY PROVIDERS



Prepared for:
National Electronic Commerce Coordinating Council

On behalf of:
Citizen Confidence and Trust Workgroup

December 2001

National Electronic Commerce Coordinating Council

The National Electronic Commerce Coordinating Council (**NECCC**) is an alliance of national state government associations dedicated to the advancement of electronic government within the states. The Council is comprised of the National Association of State Auditors, Comptrollers and Treasurers (**NASACT**), the National Association of State Chief Information Officers (**NASCIO**), the National Association of State Purchasing Officials (**NASPO**), and the National Association of Secretaries of State (**NASS**). In addition to these voting members, other governmental and private organizations participate in an advisory capacity. These associations include the Information Technology Association of America (**ITAA**), the National Automated Clearing House Association (**NACHA**), the National Association of Government Archives and Records Administrators (**NAGARA**), the National Association of State Chief Administrators (**NASCA**), the National Association of State Treasurers (**NAST**), and the National Governors Association (**NGA**). ITAA and NACHA represent private information technology companies and the financial services and technology industries.

NECCC BOARD

Chair: **Carolyn Purcell**, NASCIO, Texas CIO

Vice Chair: **Hon. J. Kenneth Blackwell**, NASS, Ohio Secretary of State

Secretary/Treasurer: **Richard B. Thompson**, NASPO, Maine Director of State Purchasing

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

NASACT	**Hon. Ralph Campbell, Jr.**, North Carolina State Auditor **Hon. Jack Markell**, Delaware State Treasurer
NASCIO	**David Lewis**, Chief Information Officer, Commonwealth of Massachusetts **Aldona Valicenti**, Chief Information Officer, Commonwealth of Kentucky
NASPO	**Dave Ancell**, Director, Office of Purchasing, Michigan Dept. of Management & Budget **Denise Lea**, Director, Louisiana Office of State Purchasing
NASS	**Hon. Mary Kiffmeyer**, Minnesota Secretary of State **Hon. Elaine Marshall**, North Carolina Secretary of State
ITAA	**Basil Nikas**, CEO, iNetPurchasing.com
NACHA	**William Kilmartin**, Accenture
NAGARA	**Terry Ellis**, Salt Lake County Records Management and Archives
NASCA	**Pam Ahrens**, Director, Idaho Department of Administration
NAST	**Hon. Jack Markell**, Delaware State Treasurer
NGA	**Thom Rubel**, National Governors Association

Acknowledgements

This white paper was prepared by the 2001 NECCC Citizen Confidence and Trust workgroup. For a list of workgroup members, please see the appendix.

CITIZEN EXPECTATIONS FOR TRUSTWORTHY ELECTRONIC GOVERNMENT:
AN ASSESSMENT AND FRAMEWORK FOR ELECTRONIC GOVERNMENT

I. EXECUTIVE SUMMARY

The timeliness of this white paper on establishing and maintaining citizen confidence and trust in electronic government has only been enhanced by the national tragedy of September 11, 2001.

More than ever before, federal, state and local public policy makers and information technology providers must be expected to develop and implement systems that are designed to meet citizen/ consumer expectations for trustworthy and secure electronic government. It is no longer simply a good government issue, but it is now a national security issue as well. Establishing and maintaining processes that are interdisciplinary from the technical, audit, policy, and legal standpoint, in both the development and operation of information systems and electronic government will go a long way towards hindering a cyber terrorist attack on government systems, records and transactions.

Even before September 11, the failure of government to establish citizen/consumer trust would have likely resulted in federal, state and local government investment in electronic government never meeting their fullest potential in making electronic government, simply government. In light of September 11, the failure to adequately develop a trustworthy and audited accountability framework of security risks, privacy risks, and operations risk in information technology could possibly lead to a cyber terrorist disaster.

As a result of September 11, there is a new environment that has been thrust upon government policy makers and citizens. Although citizen/expectations for trustworthy electronic government will likely not change as a result of September 11, the balance of interests vis a vis security and privacy will change as a result of September 11. Throughout this paper, readers

should strive to determine how the new environment regarding national security affects trust in electronic government and how best to meet citizen/consumers expectations for trust.

This paper presents no clear answer to the question of privacy versus national security, but it does clearly present the processes that government policy makers must consider to assure a successful balance of these sometimes competing interests. Simply put, readers of this paper must understand that establishing and maintaining citizen confidence and trust in government's electronic processes (technology, audit, policy, legal) are key elements in assuring the continued growth of electronic government in the wake of September 11, 2001.

This paper therefore outlines the challenge of trust, including identifying how citizens/consumers expect to develop "trust" in electronic government. Due to the unique role trust plays in the delivery of government services, Section II identifies citizen expectations for electronic government as being the same or similar to the expectations that are required to build and maintain trust in consumer and banking payment transactions. Although the services may not be the same, the consequences of a breach of trust are similar.

The remaining sections of the white paper outline on how government policy makers, information technology providers, auditors, legislators, lawyers and other professionals must work together to develop manageable and accountable interdisciplinary processes and procedures that will enable electronic government to meet citizen/consumer expectations.

Sections IV and V discuss the interaction between technology and policy in establishing trust. Section VI outlines the interdisciplinary process - audit and assessment - which is essential to citizen/consumer trust. Policy makers and information technology providers must look to audit for more than a “review of the books”. Auditors must develop processes and skills for

auditing not only governments' financial transactions, but the legal risks, operational risks, privacy risks, and security risks surrounding electronic government.

There are hardware components and software components to developing and maintaining a trustworthy security and privacy framework for delivery of electronic government. A model security policy and privacy policy for government is included within Sections IV and V. Government policy makers and information technology providers should assess security and privacy risks at such times as hardware and software is initially deployed and at any time there is a significant change or addition to the security and technology infrastructure of a government technology platform. An outline of the various hardware and software components of security trust are outlined in Section IV. Since the issues relating to privacy trust are both policy and technology, these issues are discussed in both Sections IV and V.

Section VI meets citizen/consumer expectations for trustworthy electronic government through risk assessments of software and hardware technologies vis a vis government operations and service goals. The assessment should include an assessment of legal risks (including federal, state and local privacy and security statutes, policies and industry standards, vendor contract provisions, personnel contract provisions, and assessment of legal risks for a breach of security or privacy trust), operations risks (e.g. properly trained personnel and auditable processes) and privacy risks (development of policies, legally robust system for correction and breach of policies).

This assessment can be performed by managers within the agency or contracted out. But this assessment does not negate the need for third party audit oversight of the security and privacy processes and procedures. Indeed, it is a recommendation of this paper that due to the

ever evolving information technologies that will significantly impact security trust, privacy trust and operations trust that government policy makers consider involving auditors, security penetration testers, and other assessors of security, privacy and operations in the planning stages of the deployment of new technology or anytime there is a major change to information technology.

In addition, this paper recommends that government policy makers consider legislative action to safeguard specific security risk-related technical information collected during an audit or assessment. This should be done to avoid disclosure of system features and weaknesses that could be used by external parties to exploit electronic government systems. However, because public disclosure of audit and assessment results is an important foundation for citizen/consumer trust in government, policy makers must establish a balance between public reporting and protecting electronic government systems. For example, reporting audit results could be timed to avoid disclosing security system vulnerabilities prior to correction. Supporting legislative action may be a top priority of state and local policy makers in light of September 11.

Lastly, Section VII of the paper discusses the education and outreach that is necessary to develop trust in electronic government. If there is citizen/consumer fear in the use of electronic government technology, there will be little advantage in making the case for electronic government even if the technology meets all criteria for security trust, privacy trust and operations trust. Citizen/consumers must be educated as to both the possibilities and the limitations in the delivery of government services electronically. Since the physical delivery of government services is not without security, privacy or operations risks, citizen/consumer education on the delivery of the same services electronically should be geared towards providing

citizen/consumers an ability to make an informed choice relating these different government service delivery alternatives.

II. INTRODUCTION

There are traditionally three categories of websites-"information only", "information exchange" and "fully transactional". "Information only" sites display information and there is no interaction via the Internet. "Information exchange" websites allow parties to send or receive information via the Internet, however, online payment functionality is not available. "Fully transactional" sites allow individuals to complete transactions online, including payments.

Each of these categories of websites demand increasing degrees of "trust" on the part of the citizen/consumer of electronic government services and each involves different degrees of security, privacy and operations risk for the government entity that chooses to offer government services electronically. The full realization of the economies and efficiencies of electronic government services including registrations on-line, corporate and legal filings on-line, payments on-line, sensitive communications on-line, etc. requires that the greatest number of citizen/consumers of traditional government services who wish to perform or receive the same or similar services electronically choose actually to do so.

But as a condition precedent to changing citizen/consumer habits or preferences from using for example the telephone to call a state or local government agency when that information is available on the agency's "information–only" website, or a citizen/consumer physically traveling to a municipal swimming pool to register for a swim class rather than performing that same function using the city's "information-exchange" website or physically traveling to the motor vehicle registration agency to pay and register for auto tags rather than using the state's fully- transactional website , citizen/consumers must first "feel" confident and/or trust that the expectations for private and secure communications that they have regarding on-line versus the

traditional "in person" delivery of government services or actions has been or can be met by electronic government.

The challenge of "trust" is therefore the essential element to the continued growth of electronic government and is therefore the subject matter of this year's Citizen Confidence and Trust Workgroup of the National Electronic Commerce Coordinating Council. It is the subject matter of this white paper.

First and foremost, however, readers of this paper must understand that "trust" is an intangible concept. Therefore, the challenge for policy makers and for information technology providers in electronic government is to attempt to quantify it. This is done first through understanding that "trust" results from both "assurance" and "reliance". See definition of "Trust" from the Merriam-Webster on-line dictionary, at http://www.m-w.com. The "reliance" is on the part of the citizen/consumer who "relies" on the fact that his or her expectations vis a vis electronic delivery of government services can indeed be met by government. In the absence of this reliance vis a vis electronic government, citizen/consumers will continue to use traditional government processes, such as walking, standing in line, using the telephone, etc. The "assurance" part of the definition of "trust" is the responsibility of government policy makers and information technology providers who must create, acquire and communicate to citizens trustworthy electronic government processes which can compete with traditional government service delivery processes so that those citizen/consumers who might wish to have government services received or delivered electronically actually choose to do so. Invariably, this assurance is achieved when government policy makers understand that trustworthy electronic government is an interdisciplinary of mix of technology (hardware and software), law (statutory and policy) and sound governance and operations (assessments and audits).

The continued successful deployment of electronic government services will depend on how well these government technology processes satisfy citizen/consumer expectations vis a vis electronic versus traditional delivery of government services. The focus of this paper therefore discusses and assesses how existing government processes in electronic government are or are not "trustworthy" from the perspective of meeting consumer/citizen expectations. This paper organizes this discussion of the issues impacting trustworthiness in government technology processes in the following categories: Security Trust, Privacy Trust, Audit and Assessment Trust and Education and Communication . We know that one hundred percent trustworthy process or environment is not possible for the physical delivery of government services. The same is true with the electronic delivery of such services. Consequently, what this paper discusses are risk management processes and tools that can be used by government policy makers and information technology providers to provide "assurance" to citizen/consumers that they are in fact justified in their reliance that their expectations for electronic delivery of services can be met by and through government. This is done through an examination of government's electronic "processes" – which include hardware, software, existing technology infrastructure, laws, policies, and operational reviews and audits - which all come together to provide assurance to citizen/consumers that government can indeed meet their expectations for trustworthy electronic government.

III. CITIZEN EXPECTATIONS FOR TRUSTWORTHY ON LINE GOVERNMENT

For electronic government to grow and flourish, citizen/consumers must feel comfortable that their expectations for and with electronic government will be met by government policy makers and/or information technology providers. In the absence of these expectations being met, citizen/consumers will continue to use traditional mechanisms for delivery of government services.

Therefore in each of the sections of this paper which discuss trustworthy electronic government processes in the areas of Security Trust, Privacy Trust, Audit and Assessment Trust and Communication and Education, there will always be a relation back to this Section which discusses what citizen/consumer expectations are likely to be in electronic government versus physical delivery of government services.

The following list of citizen/consumer expectations for electronic government is the result of a compilation of themes regarding consumer trust in on-line payment transactions. From one perspective, confidence and trust are developed as a result of successfully completing transactions and from another perspective confidence and trust are catalysts for consumers to begin using electronic government services. It is therefore fitting that consumer expectations regarding payment processes should be the standard for assessing how electronic government processes succeed or fail in meeting the expectations of citizen/consumers for electronic government.

The expectations of consumers in electronic payment transactions have been identified as follows:

✓ Confidentiality
✓ Reliability
✓ Consistency
✓ Predictability
✓ Availability
✓ Authenticity
✓ Integrity of information
✓ Non-repudiation
✓ Assurance
✓ No unintended/unexpected consequences

The grade that government policy makers and information technology providers receive from citizen/consumers in meeting these expectations will determine how quickly electronic government stops being called "electronic government" and simply is called "government". It is the challenge of "trust."

A. Expectation of Confidentiality

Citizen/consumers have an expectation of confidentiality in electronic government. Citizen/consumers would likely expect no more or no less public disclosure of their activities with the government over the world wide web than if such action took place over the counter. The expectation of confidentiality requires providing secure methods of transmitting information and creating and maintaining secure environments to protect confidential information that citizen/consumers are providing to government from the reach of unauthorized users. Laws are in place regarding open and public records, both in the on-line and off-line environment. However, those laws also provide a statutory mechanism for a third party to request that a public record be disclosed. Citizen/consumers expect that unauthorized users should not have access to their records in an unauthorized manner. Thus, government policy makers and information

technology providers are held responsible by citizen consumers to develop and establish a secure method to transmit information and to create secure environments. Both the establishment of a secure method to transmit information and creating secure environments require human intervention and maintenance. Thus, there is required risk management not only at the technology, hardware, software and infrastructure integration level, but also on the operations, audit and human level as well. Secure environments are called for in locations where hardware exists and where information may be stored or accessed. In addition to ensuring secure environments for the digital form of the confidential information, methods must be in place to ensure the protection of actual documents as well.

B. Reliability

Citizen/consumers expect reliability in their electronic government activities vis a vis physical delivery of the same service. Reliability is established by creating a website that is available on a regular basis to provide accurate and complete information and enables the citizen/consumer to achieve or complete the task they have initiated in the online environment.

C. Consistency

Confidence and trust will be established as citizen/consumers have positive experiences and become comfortable with the online environment in which they are conducting transactions. Consistency will result in familiarity with electronic government and in turn create confidence and trust.

Additionally, consistency refers to the citizen/consumers' expectations that their experiences will be similar at the state, local and federal government levels.

D. Predictability

Citizen/consumers should not be surprised by changes in electronic government, instead they should be notified of the changes and informed about how the changes will impact them. Citizen/consumers should be as comfortable with changes in electronic delivery or receipt of services as in the physical delivery of those services.

E. Availability

Availability of resources, information, and human contact facilitate an environment in which consumers will be confident in completing their transactions and also confident that if difficulties arise, a resource is available to resolve the issue.

F. Authenticity and Integrity

Authentication involves verification of each party's identity as well as the integrity of the message. Verifying the identity of both parties to a transaction is essential. First, the citizen/consumer must be confident in knowing that the site they are using is in fact a government site, rather than a fraudulent site. Second, the government must be able to affirmatively identify the consumer partaking in the transaction before completing a transaction or providing confidential information to the user. Third, a trustworthy transaction will ensure that information is not added to, modified, or deleted during transmission between sender and receiver.

G. Non-repudiation

Non-repudiation prevents anyone from denying that they sent certain files or data, or transacted certain business, when in fact, they did.

H. Assurance

Assurance verifies the credentials of the sender. For example, Sender A may be authenticated as Sender A, but assurance answers the question whether Sender A is a legitimate business conducting business on the Internet.

I. No Unintended And Unexpected Consequences

There are two forms of unintended and unexpected consequences that may impact the citizen/consumer and undermine their confidence and trust in electronic government. Unintended and unexpected consequences may arise as new technologies are implemented into current environments. As this happens, issues requiring government action in the legislature and/or through the implementation of technological or policy-based initiatives will arise in the electronic environment. To ensure that consumers are not negatively impacted by these developments, proactive measures, including awareness of technological changes and monitoring system functionality, must be taken to ensure seamless transitions.

The second type of unintended or unexpected consequence results from conducting transactions online. Government officials must be conscious of the amount of information that may be exchanged through the Internet and the potential effect of accidentally disclosing personal, private information. This is discussed in Section VII, Education and Communication. Government must also recognize citizen/consumer reliance on the availability and accuracy of electronic government transactions. Consequently, government must provide citizen/consumers with remedies, including legal recourse where appropriate, where there is a breach of standard protocol or the failure to meet a reasonable expectation.

IV. SECURITY TRUST

A. Hardware Technology

Creating a secure electronic government experience that meets citizen/consumer expectations regarding their choice to use electronic government versus the physical delivery of the same services requires the implementation of hardware and software technologies. Presently firewalls, extranets and intranets aid in creating secure environments for storing and providing proper access to confidential information. The successes and failures of these hardware technologies and the manner of their deployment by states and local governments goes to the issue of how hardware technology processes meet citizen/consumer expectations for "trust".

1. Firewall

Firewalls are designed as a protective barrier between the Internet and the internal network. The purpose of the firewall is to protect the local area network and internal data while permitting access outside of the network. A firewall is also used to prevent the unauthorized export of proprietary information from a network, thus controlling the flow of information in both directions.

Two important benefits that a firewall provides are blocking unauthorized users from logging into a system and serving as a security and audit point. In addition to preventing unauthorized access from "the outside world", the firewall can act as a tracing tool to locate unauthorized users attempting to gain access.

Firewalls cannot protect against information being removed from the system internally and transported elsewhere, nor can they protect against viruses and they cannot replace the maintenance required by system administrators. A sound practice to protecting extremely

confidential information is to not store the information on a machine that is connected to the Internet. Of course, this does not eliminate the problems of an internal compromise.

Most state agencies use firewalls. However, the use of a firewall, as shown above is still not without some risk to the expectations of citizen/consumers who choose to use electronic government services rather than physical delivery of the same services. One answer is education and communication of the risk management processes inherent in firewall hardware technology and let the citizen/consumer weigh the risks of compromise of their expectations versus the convenience benefits of electronic delivery of government services.

2. Extranet

Extranets are sites created outside of the local area network to provide access to specific information such as research and databases. Permission is required to gain access to the information stored on the extranet, but granting such access limits the user access to data stored on that extranet. Extranets rely on the Internet for transmission of information and as a result the security of the information being transmitted is subject to the security on the individual site. The use of the extranet provides some additional security trust to the expectations of citizen/consumers of government services. Many states have explored the use or are using extranets. For information only websites and information exchange websites, citizen/consumer expectations might be met by extranets. However, fully transactional websites still require use of the Internet. In addition, since the communication of information on the extranet still involves the Internet, the security of the site still is at issue.

3. Intranet

Intranets are internal sites used for the purpose of distributing information internally within an organization. Intranets do not provide access to the public and must be protected through the use of a firewall.

Intranets may be exceptionally useful for internal communication needs of the state governments. Citizen/consumers of government services include the actual employees of governments. Meeting government employee expectations vis a vis electronic government may be the first test to assuring citizen/consumers at large that government can deliver a trustworthy security hardware product. Of course, what is really still being discussed at this point is risk management and communication of the risk management processes as there is always the possibility of compromise of the security hardware systems, including intranets.

B. Software Technology

In addition to the hardware technology described above, software technologies offer additional security features that serve to provide "assurance" to citizen/consumers that there are processes in place in the development of not only hardware, but software as well that can meet their expectations in the use of electronic government.

1. Secret Key Cryptography (Symmetric)

✓ Confidentiality

Secret Key Cryptography is based on the use of a shared key for both encryption by the transmitter and decryption by the receiver. The message is first encrypted using a secret key and the encrypted text is then transmitted. The receiver then uses the same secret key to decrypt the message. Data Encryption Standard (DES) is the most commonly used secret-key method.

The primary weakness of Secret Key Cryptography is arranging for the sender and receiver to agree on a secret key and transmitting to both parties without a third party discovering it. The second weaknesses, perhaps the most troublesome, is that Secret Key Cryptography requires a new secret key for each new communication. A third weakness of Secret Key Cryptography is that it does not offer the benefits of authentication or non-repudiation, which results in the possibility of one party being able to claim that the other party created and sent a message when in reality they are making a fraudulent claim.

2. Public Key Infrastructure (Asymmetric)

- ✓ Authenticity
- ✓ Confidentiality
- ✓ Non-repudiation

Public Key Infrastructure is a guiding principle in Internet security that creates a secure method for exchanging information on the Internet. PKI includes the use of cryptography, digital certificates, and certificate authorities. PKI requires each sender and receiver to hold a public and private key. One key pair is used to encrypt a message and the other pair to decrypt the message.

Public Key Infrastructure has important implications for electronic government and is a critical factor in providing citizens with a secure Internet experience. In addition to providing authenticity of identity, ensuring non-repudiation, and protecting the confidential information being exchanged, PKI will provide a secure method for citizens to interact with government entities over the Internet because the private key pair is known only by the sender and need not be transmitted or otherwise revealed to anyone. The most important benefit of PKI is that the infrastructure enables key management and promotes open system transactions.

3. Digital Certificates

- ✓ Confidentiality
- ✓ Authenticity of identity
- ✓ Integrity of information

There are two types of digital certificates: server certificates and personal certificates. Server certificates are used by the hosting website and provide a secure method of enabling users to send personal information without the danger of interception or tampering through encryption. In addition, server certificates authenticate the identity of the website for the user to ensure that the site they are accessing is not a fraud. Server certificates are essential for government sites that will be exchanging confidential information with citizens.

Personal digital certificates authenticate a user's identity and can be used to restrict access to content. Personal digital certificates also provide the ability for user's to send secure email through the use of Public Key Cryptography. A digital certificate includes the holder's name, the name of the Certificate Authority, a public key, an expiration date, the class of the certificate, and the digital certification number. A citizen may obtain a digital certificate through a Certification Authority. A Certificate Authority (CA) is a trusted third party responsible for issuing digital certificates and verifying the certificate holder's identity.

Digital certificates offer a positive security solution as they eliminate the need for users to remember multiple passwords, increase security for the user as the certificate cannot be forgotten, lost intercepted, or duplicated, permits the user to send and receive secure email, and may legally be used to resolve disputes between parties in a transaction should one party deny that the transaction occurred. Digital certificates are also attractive because of their ease of use-once a digital certificate is obtained, web sites that are enabled to accept digital certificates can

authenticate the user's identity and automatically log in the user, without requiring the user to endure a registration process.

Digital certificates are superior to passwords as passwords are subject to being compromised when a user unintentionally leaves their password in a conspicuous location, uses a password that is easily "guessed", or when sophisticated hackers use programs to "eavesdrop" on systems to identify passwords stored on systems or by using software programs to "replay" passwords.

In addition to the security features offered by digital certificates, digital certificates offer benefits for both consumer and the government agency. Once a user is identified by a digital certificate, websites can be customized to the citizen's interests, allowing the states and other government entities to provide users with a unique, customizable experience.

There are maintainance issues related to digital certificates which are critical to ensuring the security benefits they offer including key management as well as the use of trusted Certificate Authorities. Key management refers to the generation, transmission and storage of digital certificates. Public Key Cryptography requires that each individual maintain the security of their private key as well as determine how to distribute their public key to individuals with whom they are corresponding. The use of Public Key Cryptography also requires the users to ensure that the digital certificates are valid, which requires contact with Certificate Authorities. Certificate Authorities are a trusted entity that serves as a depository for digital certificates who are also charged with maintaining certificate revocation lists, which identify certificates which are no longer valid. Without the use of Certificate Authorities (CA), individuals would be able to obtain a public-private key pair and claim to be someone they are not.

4. Secure Sockets Layer Technology (SSL)

- ✓ Authentication
- ✓ Integrity
- ✓ Confidentiality

Digital certificates are enabled by Secure Sockets Layer Technology (SSL). SSL, developed by Netscape, is the industry standard method used to protect Internet communication through encoding of information transmitted over the Internet. SSL is used to encrypt data for digital certification, provide server authentication, message integrity, and optional client authentication for a TCP/IP connection. SSL is built into all major browsers and web servers, and by simply installing a digital certificate SSL capabilities are activated.

SSL is layered beneath function protocols such as HTTP, Telnet, File Transfer Protocol (FTP), Gopher, and Network News Transport Protocol but layered above TCP/IP, which allows SSL to operate independently of the Internet application protocols. SSL provides authenticity, encryption, and integrity by authenticating the server and the user and because it resides "at the socket level", it is independent of higher-level applications and can provide security services to higher-level protocols such as FTP and HTTP.

5. Secure HTTP

- ✓ Authentication
- ✓ Confidentiality
- ✓ Integrity

Secure HTTP (S-HTTP) is a more comprehensive security package that includes authentication of the user's identity by the server through digital signature verification. S-HTTP uses public and private key encryption to create digital signatures but does not require a user to have a public key or register with a CA, which enables transactions to occur seamlessly because the consumer would have previously secured a key.

A serious drawback to S-HTTP is that it only functions with transactions that use HTTP, unlike SSL which works across many protocols. In light of the many protocols that may be used by eGovernment, SSL is the recommended technology.

6. Secure Electronic Transactions Protocol (SET)

- ✓ Authentication
- ✓ Confidentiality
- ✓ Integrity

Secure Electronic Transactions Protocol (SET) is a complete protocol and infrastructure that is used to enable credit card payments online. SET involves a cardholder sending payment information to a merchant, the merchant then transmits the information to the financial institution for authorization. The merchant does not actually capture the information, instead the financial institution captures the information after the merchant transmits it.

States that wish to conduct transaction online that require payment processing must consider using SET to ensure security of the transactions.

7. Encryption

- ✓ Confidentiality

There are two levels of encryption: 40-bit and 128-bit. "Bit" refers to the length of the "session key" generated by each encrypted transaction. The length of the key determines the difficulty of breaking the encryption code-therefore, the higher the number of "bits" the more secure the transaction becomes. 40-bit encryption offers a fairly high level of security, with billions of possible keys to decipher the coded information, making it nearly impossible for someone who has intercepted the information to decipher the information. 128-bit encryption offers a much higher level of encryption as there are 300 billion trillion times as many potential

keys as with 40-bit encryption, making it virtually impossible for an unauthorized party to decrypt the data.

8. Cookies

✓ Authenticity

Cookies are unique identifiers placed on a user's computer to obtain identifying information. While cookies may obtain identifying information and aid in authentication, drawbacks include "partially personalized" information as the computer may be used by more than one person and the question of determining who the actual user is when authentication is required. Many individuals also object to the placement of cookies on their computers, especially when done without notice or the opportunity to reject these cookies.

9. Secure Multipurpose Internet Mail Extensions (S/MIME)

✓ Confidentiality
✓ Integrity of information

S/MIME permits users to send confidential email messages, an important feature for citizens wishing to communicate with government agencies.

S/MIME ensures the confidentiality of email messages through encryption so that only the sender and intended recipient may read the message and provides assurance of authenticity.

C. Laws, Policies and Procedures

Laws, policies and procedures that have been enacted at the federal, state and local levels assist government policy makers and information technology providers in providing assurance to citizens/consumers that there are structures in place to add oversight and consequences for not maintaining certain standards in connection with security of information.

1. Federal Action

a. Legislative History

This legislative history is selected from portions of *The Changing Face of Federal Information Technology Security: Driving Legislation Behind IT Security in the Public Sector*, http://www.sans.org/infosecFAQ/country/fed_infotech.htm.

The Critical Infrastructure Protection Presidential Decision Directive 63, which was issued May 22, 1998, called for a national effort to assure the security of the increasingly vulnerable and interconnected infrastructures of the country. This directive required federal government action, including risk assessment and planning to reduce exposures.

i. OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources

A-130 establishes many basic considerations and assumptions, including:

- The free flow of information between the government and the public is essential to a democratic society;
- The management of Federal information resources should protect the public's right of access to government information;
- The individual's right to privacy must be protected; and
- The Federal Government must cooperate with state and local governments in the management of information resources; and

A-130 requires agencies to ensure that security is incorporated into their systems. Security controls must be consistent with the agency's enterprise architecture, and incorporate security plans that comply with federal standards.

ii. Government Paperwork Elimination Act (GPEA) (October 1998) and the Electronic Signature in Global and National Commerce Act or "E-Sign" (October, 2000)

GPEA grants legal effect, validity, or enforceability to electronic records and electronic signatures. E-Sign intends to give an electronic signature the same legal validity as pen and paper, when certain conditions are met. Over the years, dozens of states had enacted differing laws governing the use of electronic signatures. These uncoordinated actions created a legislative hodgepodge: confusing both businesses and consumers while also stunting development of e-commerce. E-Sign attempts to resolve this problem by preempting state laws other than the Uniform Electronic Transactions act (UETA) and establishing a national standard.

iii. NIST Special Publication 800-25: Federal Agency User of Public Key Technology for Digital Signatures and Authentication (October 2000)

Federal Public Key Infrastructure (PKI) Steering Committee developed NIST 800-25 to assist Federal agencies in using public key technology for digital signatures or authentication. NIST 800-25 suggests that agencies implement a public information plan, detailing the strengths of PKI technology, such as its time savings, cost savings, enhanced services and improved quality of data; costs in implementing the technology; and discuss any risks involved with its use and ways to minimize said risks. Agencies must decide if the risks are proportionate with their obligations to the public and the law.

iv. Government Information Security Reform Act (October 2000)

The purposes for the issuance of the GISRA include providing a comprehensive framework for establishing and ensuring effective controls over Federal IT resources, ensuring interoperability between Federal systems is achieved in the most cost-effective manner,

providing for the development and maintenance of controls required to protect Federal information systems, and providing a mechanism for improved oversight of Federal agency information security programs.

GISRA establishes authorities and responsibilities for Federal agencies, and directs the heads of agencies to:

- identify, use, and share best practices;
- develop an agency-wide information security plan;
- incorporate information security principles and practices throughout the life cycles of the agency's information systems; and
- ensure that the agency's information security plan is practiced throughout all life cycles of the agency's information systems.

The Act reinforces the requirements for each agency to develop and implement information security policies, procedures, and control techniques sufficient to afford security protections commensurate with the risk and magnitude of the harm resulting from unauthorized disclosure, disruption, modification, or destruction of information collected or maintained by the agency. In addition, agencies must ensure that their information security plan is practiced throughout the life cycle of each system. One of the major changes that the GISRA makes to the existing legislation is the addition of authentication and non-repudiation to the requirement of ensuring the integrity, confidentiality, and availability of information and information systems supporting agency operations and assets. Authentication and non-repudiation introduce the requirement for encryption and/or digital signatures into the security process.

Each year each agency is now required to perform an independent evaluation of the information security program and practices of that agency. The evaluation must test the effectiveness of information security control techniques for the agency's information systems

and an assessment of the compliance with Federal legislation and related information security policies, procedures, standards, and guidelines.

2. Examples of State Action

a. Tennessee

Tennessee Anytime, www.tennesseeanytime.org, is the State of Tennessee's web page which provides access to completing transactions such as renewing a driver's license online, processing a change of address, registering to vote, community information, search state databases such as real estate assessment data or business names. According to the Security policy posted on the web site, the State of Tennessee relies on SSL technology for encryption to protect consumer information.

b. Michigan

The State of Michigan recently released a new "eMichigan" portal offering citizens increased access to the state's services as well as providing the opportunity to conduct many transactions online. The security policy posted on the site does not describe the actual technologies used to provide a secure experience, it does however discuss that there are measures in place to provide security.

c. UETA

Numerous states have enacted UETA, which is not preempted by E-Sign. UETA and E-Sign have similar policy goals, including the recognition of electronic documents and signatures, which are broadly defined, as equivalent to “wet” documents and signatures. Neither UETA nor E-Sign mandate any specific security methods but they do not prohibit such methods, either. More than two-thirds of the states have adopted UETA at this time.

D. Operations and Existing Infrastructure

While hardware and software technology offer additional security features, the technologies are futile without strong operational practices to support their implementation, monitoring and maintenance. Operational measures include physical security, personnel security, and administrative security.

1. Physical Security

Access must be restricted to any location where hardware is stored. Security measures include access badges, locked cabinets to store hardware and video cameras at all access points.

2. Personnel Security

In addition to implementing a comprehensive security and audit policy, procedures must be established to ensure that those with high level access are also being monitored. Different levels of access must be granted based upon specific needs that are outlined by designated individuals. Procedures must also be in place for notifying the group responsible for granting access to delete users upon termination or when they voluntarily leave the organization.

3. Administrative Security

Administrative security refers to identification and investigation of security breaches. An effective security policy will not only create a secure environment but it will ensure over time that the procedures and technologies are effective and breaches are not occuring.

E. Recommendations for Structure and Content of Security Policy

Developing and maintaining a secure online environment should be viewed as a continuous cycle which includes risk assessment, implementation and management of a security infrastructure, training programs, regular audits, continuous monitoring and periodic

reassessment of risk and security measures. It is only from these actions taken that the expectations of citizen/consumers that there are trustworthy processes in place to justify their reliance on the security of their activities on the internet versus that in the physical delivery of services. Security can be set at any level depending upon the costs one is willing to incur. Costs include actual expenditures related to purchasing software and hardware as well as labor to maintain, update and monitor secure measures. The level of security required varies based upon the value of information being exchanged or stored. Factors that should be considered when determining the level of security include the potential cost in terms of liability and loss of public confidence.

There are two types of security-"communications security", which refers to the protection of information while it is being transferred from one system to another, and "computer security", which refers to the protection of information within a computer system. These measures need to work together with other security measures including physical security (locks on doors, access badges, and biometrics), personnel security (employee screening), administrative security (identification and investigation of security breaches), information/data security (controlling the reproduction of sensitive material), and online security (controlling access to online data).

Security measures should be designed with the above factors in mind and to protect against the most common security risks. These risks include unauthorized access (to prevent an unauthorized person from gaining access to a computer system or preventing an authorized person from using as system for an unauthorized purpose), "planting" (an unauthorized person leaves behind a mechanism to facilitate future attacks), "communication monitoring" (an unauthorized person obtaining confidential information by monitoring communication rather than "breaking in"), "spoofing" (when a domain name server accepts and uses incorrect

information from a host that has no authority giving that information; forged data is placed in the cache of the name servers and can result in users being directed to wrong Internet sites or e-mail being routed to non-authorized mail servers), service denial (access to information is denied), and repudiation (a party falsely denies that the transaction occurred).

A complete security policy would utilize the technologies detailed above to provide protection from these risks through authentication services, access controls, confidentiality measures, data integrity measures and non-repudiation services. In creating a secure environment, states must also be aware of the amount of inter-agency activities that may be taking place. For example, when a state agency collects information they may be distributing that information to other agencies. Ensuring that all state agencies maintain a standard level of security is crucial to creating a secure environment at each level of electronic government and should be taken into consideration when drafting the security policy. The security policy should also be available online for consumers to view. This goes to the issue of risk assessment by citizen/consumers leading to assured reliance that the ideas articulated in the policy are in fact being put into practice. This provides citizen/consumers with the ability to make informed choices about the site's security measures. While notice is important, ensuring that the policy is adhered to is even more important.

1. Best Practice Example-Security Policy

An exemplary security policy is attached below for reference purposes.

Example : Federal Internet Security, A Framework for Action, Appendix 4, http://www.itrd.gov/fnc/fisp_sec_contents.html

"The following is presented as an example of the type of network-specific Internet security policy that should be developed for each major Internet user community. As noted in the main body of the report, it is recommended that all agencies/organizations involved in the use of the Internet establish a policy statement, appropriate to the agency, its Internet activities, and its relationships to other agencies or organizations.

This policy example is a proposed security policy written specifically for the National Research and Education Network. It was developed by Dr. Dennis Branstad, Dr. Arthur Oldehoff, Dr. Robert Aiken, and others based on an Internet RFC written by Richard Pethia. While written for the specific Internet community, it contains basic elements that should be part of other policy statements."

SECURITY POLICY FOR USE OF THE NREN

1. OBJECTIVES

   A. This security policy has the following objectives:

   B. Establish a high level policy for protection of the National Research and Education Network (NREN);

   C. Establish a basis for further refinement of the high level policy;

   D. Establish a common foundation for the development and use of security services and mechanisms to be used in the NREN;

   E. Establish the responsibility for security among the users, managers, administrators, vendors, service providers and overseers of the NREN;

   F. Inform NREN users, managers, administrators, vendors, service providers and overseers of their security responsibility.

2. SCOPE

This security policy covers protecting the confidentiality, integrity and availability of all sensitive information and information processing resources of the NREN.

3. APPLICABILITY

This security policy is applicable to all users, managers, administrators, vendors, service providers and overseers of the NREN.

4. THREATS AND VULNERABILITIES

This security policy defines various security responsibilities and seeks to counter threats and to reduce vulnerabilities in the NREN. This is termed "Risk Management" and should be understood to encompass only cost effective means to reduce, but not remove, residual risks. This policy specifically informs users and overseers that all threats and vulnerabilities WILL NOT be removed. No guarantees or warranties for confidentiality, integrity, and availability will be explicitly or implicitly given through this policy.

5. PRINCIPLES

The following principles should be followed in using this policy:

A. Personal Accountability: Individuals are responsible for understanding, respecting and following the security policies of the systems (computers and transmission facilities) they are using and are personally accountable for their behavior and actions.

B. Authorized Use: Authorized use of the NREN is defined as those activities authorized to be performed by an individual in accordance with the "NREN Acceptable Use Policy". Unauthorized use includes any activity that is illegal, disrupts authorized use, compromises privacy of other users or destroys the integrity of information or processing capability.

C. Reasonable and Prudent Precautions: Each person using or supporting use of the NREN shall take reasonable and prudent precautions to assure the availability and integrity of its resources and the confidentiality of information known, or assumed, to be sensitive to disclosure to unauthorized persons.

D. Cooperative Protection: All persons using or supporting use of the NREN shall cooperate in providing and using appropriate protection its resources and information.

6. RESPONSIBILITIES

This section defines basic responsibilities for security by those groups of organizations and individuals as identified in the scope of this policy. The responsibilities are general and are not based on existing or planned protection technologies or practices.

A. Users

Authorized users of the NREN are responsible for :

U1. Knowing and complying with relevant Federal and State laws, NREN policies, organizational codes of ethics, and acceptable security practices for the systems they use;

U2. Employing available security mechanisms for protecting the confidentiality and integrity of their own information when required;

U3. Advising others to follow U1 and U2;

U4. Notifying a system administrator or management if a security violation or failure is observed, detected or suspected;

U5. Not exploiting security vulnerabilities;

U6. Supplying correct and complete identification as required by authentication or access control processes in the network;

U7. Using the network only for authorized purposes in a cooperative, legal, ethical and responsible manner;

U8. Using standard security mechanisms to promote interoperability when available and to the maximum extent possible.

B. Management (Multi-user Hosts and Facilities)

Multi-user host computer and facility managers are responsible for:

M1. Implementing cost effective "risk management" procedures, security mechanisms, protection features for the hosts and facilities they manage;

M2. Providing trusted personnel to support the security specified in M1;

M3. Implementing management directives and awareness programs for the administrators and users of their hosts and facilities.

C. System Administrators

System administrators (or their designated personnel) are responsible for:

S1. Applying, monitoring and auditing the security procedures, mechanisms and features available on the hosts or facilities under their control;

S2. Advising management on the workability of existing policies and technical provisions of the system, including recommending improvements for security purposes;

S3. Securing computer systems and subnetworks within the facility/site and the interfaces to outside networks;

S4. Responding to emergency events which are or may be affecting their hosts or subnetworks in a timely and effective manner;

S5. Employing available and approved monitoring and auditing tools to aid in the detection of security violations and actively participating in educating and counseling users who violate security;

S6. Remaining cognizant of NREN security policies and recommended practices and, when appropriate, informing local users and advising local management of changes or new developments;

S7. Communicating and cooperating with administrators of other sites connecting to the NREN and with emergency response centers for the purposes of information exchange and responses to perceived threats, increasing vulnerabilities or observed security violations;

S8. Judiciously exercising the powers and privileges inherent in their duties, appropriately considering the security of the NREN and the privacy of the individuals using it.

D. Federal Networking Council

The Federal Networking Council (FNC), serving as the principal body coordinating the activities of federal research and education network organizations, is responsible for:

N1. Developing, approving, maintaining, and promulgating an NREN security policy;

N2. Recommending, approving and promulgating standards for interoperable security services, mechanisms and procedures for the NREN;

N3. Establishing rules for accepted and authorized use for selected (e.g., federal) portions of the NREN;

N4. Coordinating with federal agencies, educational institutions, private organizations and special interest groups (service providers, vendors, system developers, emergency response centers) regarding security of the NREN;

N5. Interacting with appropriate national and international standards organizations developing security standards which may be relevant to the NREN;

N6. Preparing reports or input to reports to executive organizations and congressional committees responsible for oversight of the NREN.

E. Vendors and System Developers

Vendors and systems developers are responsible for:

V1. Employing sound development and distribution methodologies for implementing or providing secure systems, subnetworks and networks as specified in procurement or management documents supporting the NREN;

V2. Seeking technical improvements to security of their products and services appropriate to the policies and specifications of the NREN;

V3. Correcting security flaws discovered in existing products and making the system administrators aware of the availability of product improvements;

F. Computer Network and Service Providers

Computer Network and Service providers are responsible for:

P1. Providing network security services and mechanisms as specified in procurement or management documents and making information available to managers, administrators and users on how to administer and use these security provisions;

P2. Seeking technical improvements to the security of the NREN that is within their areas of responsibility;

P3. Cooperating with the FNC in providing appropriate network availability and integrity assurance capability.

V. PRIVACY TRUST

A. Introduction

Meeting citizen/consumer expectations regarding trustworthy processes in the area of security may not in and of itself lead to the assured reliance on the part of citizen/consumers that will lead to increased usage of electronic government, unless citizen/consumers are also knowledgeable and understand what and how the information that is gleaned from their activities in electronic government is gathered, held and used, in other words – Privacy Trust.

The public's concern with online privacy is growing at an exponential rate. Collection of data about individuals has always invoked issues of privacy. However, online technology increases the concern as it allows for storage of more data, faster and easier than before. In addition, it allows for easier manipulation of that data and cross-referencing at heretofore unimaginable speed. Most significant of all, in the online world, data collection can occur without the knowledge of the citizen/consumer (e.g. cookies).

Collection of data without consent is the biggest issue privacy advocates are raising with online websites. Such concerns have even greater implications when it is potentially government which is capturing information without the knowledge or consent of citizen/consumers. Contrary to the "old days" of warranty card registration, now data can be collected about individuals without their permission or active participation. As citizen/consumers and other users customize their web browsers with personal information, they do not always realize that this information can be accessed from Web sites they are visiting and then stored in the Web site's database.

When people surf the web, they have a general expectation of anonymity, because they are not physically observed by others on the web. Yet, many people do not realize that they leave behind transactional data that can provide a profile of an individual's online life. This is made possible by technologies called cookies, which are written directly onto an individual's hard drive to enable web sites to surreptitiously collect information about that individual's online activities and store it for future use.

The Internet accelerates the trend toward increased data information collection which is already evident in a citizen/consumer's offline world. The data trail, known as transactional data, left behind as individuals use the Internet is a rich source of information about their habits of association, speech, and commerce. This data trail is particularly troublesome when used by others in electronic government for purposes unrelated to the initial collection of the information. Yet is such information a "public record" subject to open disclosure and potential use by third parties unrelated to the electronic government transaction? Transactional data, click stream data can include the Internet protocol address ("IP address") of the individuals computer, the browser in use, the computer type and what the individual did on previous visits to the website or perhaps to other web sites. This data may, or may not be capable of identifying a specific individual. Some of the data collected is essential (like the phone number that connects a calling party to the intended recipient), while other information collected serves non-essential purposes. It is the collection of this non-essential data that is most alarming to the development of citizen/consumer privacy trust in electronic government processes. It is this risk of breach of the citizen/consumer's expectations of electronic government versus continued to use physical delivery of services which must be addressed by government policy makers and information

technology providers. The status and methods for how this is done is the subject matter of this chapter.

This increased data collection is making consumers fearful of the use of their data after they have consummated a transaction with a Web site. They worry about who can see this data, who gets this data, what it is combined with and what it is used for. In particular, citizen/consumers are concerned with the collection of personally identifiable information and not aggregate data. Web sites respond to this concern by explaining that the more information that is available to Web site operators, the more they can help tailor the user's online experiences in ways the user finds worthwhile.

In order to preserve citizen/consumer's privacy trust, electronic government Web sites and government policy makers and information technology providers must provide assured reliance that there are trustworthy processes in place and those processes are being implemented so as to meet the expectations of citizen/consumers who might wish to participate in electronic government. As discussed at the end of this chapter, such assured reliance results from government providing assurance to citizen/consumers that their Web sites fully comply with five key processes or requirements that set forth the privacy relationship between government and the citizen/consumer. These requirements are notice, choice, access, security, and enforcement.

B. What Constitutes Privacy Trust In The Government Sector?

Privacy on a Web site, whether it belongs to a commercial, vendor, individual, or government entity, is a serious concern among citizen/consumers. As of September 15, 2000 only 5% of government Web sites contained some form of security policy, and 7% have a privacy policy. Recent polls indicate that public concern about online privacy is the number one reason that consumers are not currently using the Internet. A substantial majority of U.S.

citizen/consumers do not go online, and a substantial number of citizen/consumers who do use the Internet choose not to purchase goods sold through Web sites that do not disclose their privacy policies. Recent survey data indicates that 92% of citizen/consumers are concerned (67% are very concerned") about the misuse of their personal information online. This apprehension likely results in fewer online sales due to lack of confidence in how personal data will be handled in the private sector. In the public sector, there is an even higher privacy standard due to the potential that "trust" breached in the public sector might lead to mistrust in government processes in general. Indeed, surveys show that citizen/consumers most concerned about threats to their online privacy are the least likely to engage in online commerce. This reinforces the importance for government Web sites, government policy makers and information technology providers to take leadership steps to provide assurance to citizen/consumers that their expectations regarding their privacy when transacting government services on line is commensurate with costs of continuing to perform the same services through the physical delivery of government services.

Trust is the foundation of a sustainable relationship between the web user and the web site owner whether that owner is a company or government. Violate this trust, and it is difficult and costly to re-establish. Therefore, it is critical for government to establish formal website privacy policies and proactively monitor actual practices--to help avoid Web site privacy breaches. Only by building and maintaining their user's trust, can government truly maximize the opportunities afforded by the Internet.

At its essence, trust is a Web site doing what it said it was going to do and having the processes in place to provide assurance that reasonable expectations regarding the online experience are met. Trust is critical to minimize unintended consequences of government action

and to gain consistency in the marketplace in order to achieve predictability of experience. In order to facilitate a trusting experience for the citizen/consumer, the citizen/consumer must have assured reliance on the Web site. The assurance must precede reliance and take the form of an assurance that the system is in fact reliable.

C. Laws, Policies And Procedures

Presently, there is no comprehensive federal or state legal scheme to impose governmental regulation of privacy or security issues on the World Wide Web. Many legislators are concerned that any regulations would be inherently territorial, they would be unable to adjust to the fast moving web and any regulatory solution would try to impose one-size fits all requirements. In spite of this, there are initiatives on the state and federal level to promulgate new regulations.

Some states have undertaken special treatment for sensitive information that is submitted or stored online. Maine for example, generally forbids any sale or disclosure of mailing lists or account information of credit card holders to a third-party without an explicit opt-in provided by the consumer. Florida, and Hawaii also generally have opt-in schemes for the dissemination of credit card lists. Oregon has a law limiting access to driver's license information. And, a Colorado court has recently upheld the right of the judiciary to restrict access to judicial records to those who are physically present at the court site. Texas adopted a rule, requiring the home pages of all state web sites and those of any new, or changed key public entry points to include privacy policies which address certain areas. This can be viewed at http://www.state.tx.us/Standards/S201-12.htm. Many state statutes protect the privacy of medical information by providing patients with a general right of access to their medical records and protection from disclosure of medical records by licensed health-care providers. There are

also state common law schemes that behoove state government Web sites to protect individuals right to privacy, or face the possibility of a lawsuit.

A more detailed analysis of existing and proposed federal and state online privacy legislation, policies and practices can be viewed at (_____), a paper prepared by the E-Sign Policy Work Group and published by the NEC3.

D. Operations And Existing Infrastructure

- The Platform for Internet Content Selection (PICS) is a set of technical specifications that enables consumers to find appropriate content and to avoid content they consider inappropriate or unwanted, either for themselves or for children. The PICS specifications provide ratings on a web site's content.
- Crowds provides anonymity to individuals surfing the Web by mingling their request for access to Web sites with those of others web surfers. This enables the identity of the requester to remain hidden.
- Onion routing uses the decentralized nature of the Internet coupled with public key encryption to provide privacy protection for Internet communications. The onion routing uses technology to protect an individual's identity.

E. Application Of Hardware Technology

Some technologies limit the collection of personally identifiable information. For example there are anonymizers in the marketplace such as crowds and onion routing which provide consumer with the ability to cloak one's identity. These technologies may be useful to protect against the accidental disclosure of social security numbers, credit card numbers and bank account numbers. One drawback of this type of technology is that it makes it more difficult

for Web sites to provide online services to their consumers. There are also certain collective security issues that mitigate against anonymizers.

Another technology impacting privacy is the Platform for Privacy Preferences Project (P3P). This is a standard developed by the World Wide Web Consortium that enables Web sites to list privacy practices in a format that can be retrieved automatically and interpreted easily by user agents. P3P agents allow users to be informed of site practices (in both machine and human-readable formats) and to automate decision-making based on these practices when appropriate. P3P allows customization of privacy preferences. It is unobtrusive because it interrupts a transaction only when there are privacy discrepancies. The complete list of sites using P3P can be viewed at http://www.w3.org/P3P/compliant_sites

F. Application Of Software Technology

A technology of particular importance is payment mechanisms that preserve the consumer's anonymity. In particular digital certificates could be designed to limit the instances in which identity is used as a broad substitute for specific traits and abilities. For high privacy risk transactions, there is the option of anonymity. For example, there are internet payments systems that would have the purchaser’s bank be unable to link the transaction to the individual purchaser. Digicash is a example of this type of payment mechanism that provides cash-like anonymity to individual users.

The market for privacy protection is growing and companies are responding with a host of technological tools. These technological privacy tools can be divided into two types: those that protect or shield a browsing consumer's identity, and those that help the consumer negotiate what information he or she wishes to share.

- Anonymizer technologies such as anonymizer.com and Zero Knowledge Systems give a consumer anonymity on the Web.

- Infomediaries allow a consumer to exercise choice in the types of personally identifiable information that is shared each time a Web site is visited. A consumer can create a personal profile that enables the technology to negotiate the release of information specified by the consumer. This is especially relevant in today's Internet environment. According to one survey, 92% of Internet users would be uncomfortable (67% "not at all comfortable") if a Web site shared their information with other organizations. An overwhelming majority of surveyed consumers (88%) want sites to ask permission before sharing their personal information with others.

- Alladvantage.com acts as an agent on behalf of consumers to create a market for the use of their information without consumer's losing control over their information.

- Persona by Privia Seek allows a consumer to surf anonymously and sell his or her specified, personally identifiable information in exchange for discounts.

All of these technologies distinguish the citizen/consumer's need to shield their personally identifiable information versus harmless information such as demographic data and aggregate data (e.g. any information that can not be linked to a specific, identifiable individual).

G. Assessment Of Current Efforts To Provide Privacy Policies And Statements On Portals

1. Recommended Structure And Content Of Privacy Policy

It is critical for government policy makers to take the time to draft a privacy policy. Survey data shows that an overwhelming majority of citizen/consumers believe that it is "absolutely essential," or "very important" that a site display a privacy policy, and to explain how

personal information will be used before citizen/consumers provide information or make a purchase.

The federal government's Web site (first. gov) places its privacy link in a highly visible position. The link is placed on its navigation bar at the top of the page, and right next to the main page link. Additionally, the policy itself is very clear. It says, "We will collect no personal information about you when you visit our website unless you choose to provide that information."

In order to provide assurance that citizen/consumer expectations for their electronic government experience have been met, state and local governments standards for such assurance require development of privacy policies. These policies are sometimes even required by law. The federal government has adopted a policy on its web sites that cookies should not be used at electronic government sites, or by contractors when operating Web sites on behalf of agencies, unless, in addition to clear and conspicuous notice, the following conditions are met: 1.) a compelling need to gather the data on the site and 2.) there is an appropriate and publicly disclosed privacy safeguards for handling of information derived from cookies.

H. Recommended Structure And Content Of Privacy Statement

A privacy statement must be drafted with the reader in mind. A reader will be more likely to read a statement that is written in a concise (a policy should not run longer than several pages), and clear fashion. The statement must enable citizen/consumers to get a general idea of the government site's privacy policy without being required to read through legalese, and technical jargon.

When drafting a privacy statement, there is a tension between providing full and accurate disclosures about a site's information practices, and providing short and easily understandable

disclosures that are simpler to read. To manage this tension, government policy makers should draft a short privacy statement with links under each section of the statement to a complete description of the overall statement (e.g. descriptions of technical information in web logs, links to governing laws etc.).

Many Web sites in the private sector sites write their statements in general, privacy protective language, only to reveal further in the policy multiple exceptions to the general rule. Other sites use ambiguous, or misleading language in their statements. For example, some sites use ambiguous language to describe how consumers can exercise choice. Here, the use of ambiguous language undercuts the value of offering citizen/consumers choice in the first instance.

Many privacy statements assert that the Web site reserves the right to make changes to its information practices in the future. If the site makes a change in the future, it is possible that new, inconsistent policies may be applied to previously collected information. This may be an unfair and/or, deceptive trade practice. Government policy makers should keep this in mind when making changes to their statement. Government websites which alter their privacy statements should consider having the alterations be prospective only. At the very least, if a government website changes their privacy statement, the site should inform consumers whose information they have collected of any material changes in their information practices.

When drafting a privacy statement for a web site, the citizen/consumer as reader will be better informed about a government's privacy practices if specific language is used. In addition, the specific language should incorporate the same terms as other agencies in the state. Moreover, links to a privacy policy should be prominently displayed on a site's home page, and

on every page on which personal information is collected. Ideally, the location of the link should be consistent for the site and all other eGovernment sites in the state.

The privacy policy should also contain links to the text of laws with which the site must comply such as the Freedom of Information act, or sunshine laws, or public records laws.

- The state of Washington has put out a memo giving readers a step-by-step explanation on how to draft a privacy statement. This can be viewed at http://www.wa.gov/dis/e-gov/architecture/FinalPrivacyModel.htm

1. Best Practice Examples

a. Privacy Policy

- The privacy organization, the Internet Alliance drafted a white paper exploring what a Web site needs to put into a privacy policy. This white paper titled "Building Consumer Trust and Confidence in the Internet Age" is located at http://www.internetalliance.org /policy/trustwp.html
- The Federal Office of Management and Budget has a memorandum on privacy policies on Federal Web sites located at http://www.whitehouse.gov/omb/memoranda/m99-18.html; with an attachment located at http://www.whitehouse.gov/omb/memoranda/m99-18attach.html
- Michigan Department of Attorney General has put out "A Guide to Privacy Policies" that is located at http://www.ag.state.mi.us/inet_info/priv_guide.pdf

b. Privacy Statement

The following are examples of privacy policies that discuss notice, choice, access, security, and enforcement in a clear and concise manner:

- The FTC's privacy policy is located at http://www.ftc.gov/ftc/privacy.htm

- The federal government's Web site has a privacy policy located at http://firstgov.org/top_nav/privacy. html/?ssid=996064665671_172
- The state of Utah's privacy policy is located at http://www.utah.gov/privacypolicy.html
- In the commercial sector, eBay has a well-written privacy policy located at http://pages.ebay.com/help/com
- North Carolina's privacy policy is located at http://www.ncgov.com/asp /subpages/privacy_policy.aspmunity/png-priv.html
- The state of Connecticut's privacy policy is located at http://www.state.ct.us/privacy.htm
- The state of Michigan's privacy policy is located at http://www.ag.state.mi.us /priv_plcy.htm

2. Develop A Written Privacy Standard

There are five actions that government policy makers can take to provide the assurance to citizen/consumers that can evidence government's intention to meet citizen/consumer expectations vis a vis privacy in the citizen/consumer's choice to use electronic government versus physical delivery of government services.

The five elements or actions that government policy makers can take are in bold, and each one is followed by a discussion of what the elements entail in order to be satisfied.

- **Notice: Provide clear, conspicuous notice of your information practices**.

  Citizen/consumers must be given notice at the time data is collected of:

  - what kinds of information are being gathered;
  - how that information is being collected (directly or through non-obvious means such as cookies);
  - whether requests for information may be refused (if so, what are the consequences);

- the uses that will be made of that data;
- the persons or entities who will receive or have access to that data;
- whether other entities are collecting information through the site; and,
- whether an individual may limit the dissemination, or use of collected personal information.

Additionally, the Web site should contain methods for citizen/consumers to contact the site over the telephone, in writing, or via facsimile. Also, it should clearly define what is "personally identifiable information." Finally, the site must provide notice to citizen/consumers before the collection of any information, and prior to any material changes in information practices.

- **Choice: Offer consumers a choice regarding how personal identifying information is used**.

Web sites should offer consumers a choice regarding how their personal identifying information is used beyond the information's use to consummate a transaction. The choice would encompass internal secondary uses (e.g. marketing back to consumers) and external secondary uses (e.g. disclosing data to other entities). Data collectors should afford citizen/consumers an opportunity to consent to secondary uses of their personal information.

The privacy policy should clearly explain how a citizen/consumer can exercise choice over the use of his or her information. This approach is preferable over a policy simply declaring that a citizen/consumer's personal information will not be shared without his, or her consent. Also, the policy should include a mechanism allowing citizen/consumers to delete, or deactivate personal information from the site's database upon request.

When deciding how to provide choice to consumers, government policy makers have the option of choosing between an opt-out approach, or an opt-in approach. The opt-out approach allows an electronic government site to specify the terms of choice (i.e. what information a consumer may direct not to be disclosed or used for a secondary purpose) and puts the burden on the citizen/consumer to communicate his or her choice to the information gatherer. Under the opt-in approach, electronic government sites must obtain affirmative consent prior to disclosure or secondary purpose use. An opt-in rule may be costly and prevent the sites from providing customized services and features that citizen/consumers want.

To provide reasonable assurance that there are processes in place that protects a citizen/consumer's expectation of privacy in online government, it would be safer in general to provide consumers with an option to opt-in to any disclosure of information. Specifically, an opt-in approach should be used when the site wants to disclose sensitive information, while an opt-out approach should be used when the site wants to disclose less significant information. For example, some information, such as medical data, is so sensitive that a citizen/consumer's express affirmative consent should be required for any secondary use or disclosure including sharing among affiliated governmental or non-governmental entities. Disclosure for secondary purposes of other sensitive personal information, such as an individual's social security number, income purchasing history or religion, should also hinge on the citizen/consumer exercising their opt-in choice. Whatever choice a government policy maker makes, the opt-in or opt-out choice should always be clearly presented, easily located and simple to use.

Secondary uses or disclosures of information that provide significant societal benefits may be exempted from the requirement of consumer choice. Possible examples of such

exemptions include disclosures made in response to judicial process, law enforcement purposes, and for fraud detection and prevention.

- **Access: Offer consumers reasonable access to information Web sites have collected**.

Citizen/consumers need to be provided with access to information they have submitted to Web sites.[1] This will allow consumers to review, and where necessary, modify the information collected in order to correct any inaccuracies in the information collected.

Due to the extraordinary range of online data processing activities at sites, it may not be possible to provide citizen/consumers with access to *all* data about themselves. For example, a website may automatically record navigational, or clickstream rates as an individual moves from page to page on a site. This is done for either statistical purposes, or to automatically personalize the initial pages presented to the visitor based on the visitor's historical use of the site. Such information is processed automatically and changes over time. Web sites need to be provided with leeway to make their site efficient and useful to citizen/consumers.

Additionally, a site that allows a consumer to access all data regarding themselves could implicate additional privacy risks. The more data is readily available at the Web site by the name of a consumer, leads to increasing amounts of identifying data that must be collected in order to authenticate that the person requesting access to the information is indeed the proper data subject.

[1] Interestingly, the advisory committee to the FTC's 2001 report "heard estimates from Web companies that less than one percent of customers who are offered access actually take advantage of the offer."

As a result, only data that affects the fundamental freedom of a citizen/consumer, or provides them with more than mundane benefit should be capable of being accessed by the consumer. A Web site can balance the consumer's desire for access and the consumer's desire for privacy by imposing a policy of reasonable access to information. Reasonable access to information can promote accuracy, and safeguard against errors or fraud in some circumstances.

- **Security: Take reasonable steps to protect the information you collect from consumers**.

Security is a process; no one static standard can assure adequate security because the threats to the security of a site are constantly evolving. Still, government policy makers need to take measures to protect data from destruction, loss, misuse, or alteration. These measures involve both managerial and technical measures. In addition, the measures should be appropriate to the circumstances (e.g. health records of individuals must be afforded greater security than the typical information submitted).

An electronic government web site need not have to fully describe the security measures taken to protect consumer's information. Detailed disclosures could confuse citizen/consumers and invite security breaches. Yet, some disclosures of security measures are necessary to enhance consumer's trust in the privacy of their information. Specifically, Web sites should post disclosures about security that specifically address the fact that measures are taken after receipt of consumer's personal data.

In particular , Web sites should disclose basic data security systems, and retention processes. This could include an explanation of how third parties must safeguard the information and an assurance about the integrity of security measures. For example, a Web site

should discuss how they make employees aware of their security policy and practices: is access to data limited; how do employees gain access to data; do they periodically review web security?

- **Enforcement: provide consequences for deviation from practice**.

A description of enforcement mechanisms is another tool that can be used to augment a citizen/ consumer's confidence and trust in a site. Enforcement mechanisms are designed to ensure compliance with an objective code of personal information practices and to obtain redress for violations of that standard. These mechanisms can be accomplished through self-regulation or legislation.

VI. AUDIT AND ASSESSMENT TRUST

A. The Elements of Audit and Assessment Trust

Before state policy makers and information technology providers can meet citizen/consumer expectations for trustworthy electronic government, citizens/consumers must be confident that those interdisciplinary policies, actions, processes, and procedures outlined in prior sections of this paper have been implemented by government policy makers and are in fact being applied.

When new electronic government services are brought on-line or when there is a significant modification made to hardware or software technology, this confidence is initially achieved through an assessment of the new or substantially modified systems for security trust, privacy trust and operations trust. These assessments can be performed by either governmental employees, or independent reviewers whose "assessment" operates as assurance or a "seal" that the processes leading to security trust, privacy trust and operations trust have been examined by the agency implementing the new or substantially revised technology.

These assessments, however, do not negate the need for and the responsibility of electronic government policy makers to provide for a vigorous third party performance and compliance audit of existing technologies and processes. This audit, like an assessment, will sometimes involve security vulnerability and penetration testing. Several states are providing authority for both the managers of information systems and their state auditors to perform security vulnerability and penetration tests as part of their respective duties. The states that are providing such authority have also typically included exemptions of the detailed results of such security vulnerability and penetration tests from being included as part of the state's public records law. States may consider whether and how the results of all information technology security testing should be exempted from state's public records laws regardless of whether the testing is performed by IT managers or auditors. This is particularly needed after September 11, 2001.

In addition, given the ever-evolving interconnectivity of new technologies linking the information resources of one state agency with other agencies, it may increasingly become necessary to involve auditors at the initial stages of the development of the new technology in order to effectively perform their statutory audit functions. This may involve states hiring or providing specialty training of auditors at the initial stages of new technology development. It may also involve providing an opportunity for participation by either IT managers and state auditors in the engagement of third-party auditors, assessors or seal providers. Involvement of state auditors in the IT development process will likely assist IT managers in building sound control systems and avoid audit findings from their state auditors. Early participation will also likely provide an opportunity for IT managers to educate auditors on specific information technology issues.

Lastly, these assessment and audit processes must be communicated to citizen/consumers in a way that leads to reliance that the processes implemented by government policy makers for electronic government lead to "trust". This includes assuring that citizen/consumers using electronic government services have a legally robust system that can prevent parties from successfully repudiating electronic transactions, messages and records.

B. Risk Assessment

While an assessment and audit structure is developed that can manage oversight of information technology within and across state agencies, those charged with running the state's IT program should also develop a risk assessment program to weigh the appropriate levels of oversight and costs versus the impact that failures in technology and technology processes might have on security trust, privacy trust and operations trust. This program should identify, quantify and compare the various levels and types of risk in electronic government versus the potential harm that might accrue due to breaches in security trust, privacy trust or operational trust. This risk assessment program, however, is only one part of the interdisciplinary information technology trust program. The National Electronic Coordinating Council has published a Risk Assessment Guidebook for E-Commerce/E-Government which provides guidance in performing an interdisciplinary risk assessment.

The goal is to have the appropriate processes in place that can lead to citizens/consumers reliance that the risks versus the benefits of electronic government compare favorably to the risks versus the additional burdens for physical delivery of those same services.

VII. CITIZEN/CONSUMER COMMUNICATION AND EDUCATION

Another practice that governments could implement to instill citizen/consumer confidence and trust in the use and deployment of electronic government services is to communicate with its citizens on the importance of issues impacting trustworthiness in government technology processes. While many surveys and other public opinion research efforts have identified that Americans in general, and Internet users in particular, are worried about privacy and security violations that could occur online, these same studies reflect that most people do not follow the issues closely.[2] Most people do not understand what personal information is typically collected by public or private web site operators and how that information is used, or what security measures are available and routinely employed on such web sites. Nor are consumers generally aware of some of the benefits the public derives from the use of certain online data collecting practices and technologies. Consequently, the public is generally concerned but uninformed about these issues. Therefore, the public's perception of its ability to interact safely and confidently over the Internet, whether in the private or public arena, is distorted by this lack of knowledge of the facts surrounding these issues. This provides the government with a prime opportunity to impact the level of trust that citizens and other consumers of government services have in the use of electronic government processes, through the implementation of citizen outreach and educational initiatives.

An example of government efforts to open a dialogue with and educate the public about issues that impact trustworthiness in government technology processes is found in the work of the Federal Trade Commission (FTC). Starting in 1995, the FTC began conducting workshops, hearings, surveys and studies of online privacy and related issues, practices and concerns that

consumers identified as important to them when using the Internet.[3] As a result of these efforts, the FTC has taken a number of approaches to address consumer/citizen online privacy interests. One such approach has been to educate consumers and businesses alike about the importance of personal information privacy. The FTC maintains a web site that contains a host of articles addressing the online collection of personal information and why it is important to protect the privacy of one's personal information.[4] The FTC has partnered with various state Attorney General's in providing this information to the consumer public. In this regard, the National Association of Attorneys General (NAAG) supports the use of educational programs to enlighten both consumers and businesses as to the laws, choices and protections relevant to this issue, and the responsibilities each party in an online transaction shares to ensure a safe and secure online experience.[5] Likewise, the National Governors Association (NGA) has suggested that state Governors take the lead in educating the public in the significance of both public information and personal privacy in the e-Government environment.[6]

Other examples, where government resources have been dedicated to informing and educating consumers and citizens about the importance of online privacy issues, can be found at the U.S. Department of Commerce National Telecommunications and Information Administration's web site, http://www.ntia.doc.gov/, and at the Department of Education's "Parents Guide to the Internet", http://www.ed.gov/pubs/parents/internet/. Both of these agencies provide citizens with clear and easy to understand information on what and how personal

---

[2] Ryan Sager, *Public: Take Our Privacy, Please*, Wired News, May 9, 2001, at www.wired.com/news/privacy/0,1848,43657,00.html.
[3] *Privacy Online: A Report to Congress* at 2 (Federal Trade Commission June 1998).
[4] *Privacy Initiatives*, Federal Trade Commission at www.ftc.gov/privacy/index.html.
[5] *NAAG Privacy Subcommittee Report: Privacy Principles and Background*, NAAG Spring Meeting, March 13-16, 2001.

information is typically collected and used by web sites and online service operators, and how the Internet can be used to best serve a consumer's privacy interests.

Some state agencies that have already implemented outreach and educational initiatives on this issue include the Kansas Insurance Department, which provides citizens with ways they can protect their health information privacy.[7] The California Department of Consumer Affairs provides consumers with privacy protection strategies for use on the Internet through online publications and fact sheets and a toll-free hotline.[8] Likewise, the New York State Attorney General maintains a web site link and consumer hotline, and publishes a pamphlet, through which citizens are provided with detailed information about how to protect their privacy in cyberspace.[9]

Governments could also take a lesson from various private businesses and not-for-profit organizations that have pursued online campaigns to educate consumers about privacy interests. DoubleClick, a company that provides digital marketing and Internet advertising technology and services to commercial web sites, hosts a web site of its own that is devoted to consumer privacy education.[10] Among other things, DoubleClick provides information concerning consumer benefits derived from web site personal data collection and sharing practices, like free-of-charge services and personalized web site visits. Additionally, certain non-profit organizations like the

---

[6] *Privacy – Building the Public Trust*, National Governors Association, June 20, 2000 at www.nga.org/Pubs/IssueBriefs/2000/000620Privacy.asp.
[7] http://www.kinsurance.org/other/privacy/privacyflyer/privacyflyer.html.
[8] htpp://www.dca.ca.gov/press_releases/000210.htm.
[9] http://www.oag.state.ny.us/internet/privtips.html.
[10] www.privacychoices.org.

Privacy Rights Clearinghouse and Consumer.net, provide consumers with links and helpful information on how to protect their personal privacy in the online environment.[11]

Lastly, citizen/consumers must be informed and knowledgeable on the ways that open records laws may provide access to information electronically that may not be readily available through non-electronic means. This potential conflict of openness versus privacy is one that will likely be the subject of legislative debate as electronic information becomes more readily available and utilized. This debate should occur sooner rather than later in light of the events of September 11 and the availability of such information to the universe of internet users —foreign and domestic.

VIII. APPENDIX

Citizen Confidence and Trust Workgroup Members

John Aveni	J. Kenneth Blackwell	Tom Bossie	Ralph Campbell, Jr.
Frank M. Dean	David DeStefano	Christina Dorfhuber	Bonnie Ettinger
Ed Fraga	Scott Frendt	Danielle Germain	Dan Greenwood
Michele Grisham	Ray Headen	Marc Hiller	Jerry Johnson
Mary Kiffmeyer	Michele Kryszak	Wanda Lairson	Kara LaPierre
Brandon Lenoir	Alia Mendonsa	Kathy Minchew	Bob Moriarty
Basil Nikas	Darby Patterson	Nancy Rainosek	Leslie Reynolds

[11] http://consumer.net/index.asp; http://www.privacyrights.org/.

Matthew Rosenthal	Eric Seabrook	Bill Sullivan	Martin Vernon
Tom Wagner	Karen West	Lynne M. Wolstenholme	