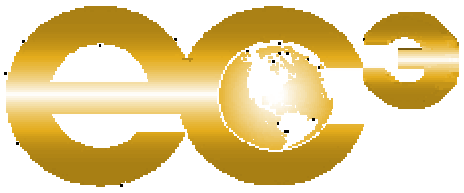
Building Citizen Trust and Confidence with Web Site Branding



Exposure Draft

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 State Chief Administrators (**NASCA**), 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**, Nebraska 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 web site branding and seal project team created by the 2001 NECCC Citizen Confidence and Trust workgroup. The project team included the following people:

Chair: **Nancy Rainosek**, Office of the Texas State Auditor
Mark Hiller, New York State Office for Technology
Jerry Johnson, Senior Policy Analyst, Texas Department of Information Resources

For a complete listing of workgroup members, please see Appendix C.

Outline

I. Overview

Government entities at all levels are seeking to meet citizen demand for providing access to government information and services on the Internet. However, just as with traditional paper based services, each citizen has a right to expect governments to protect their interests. This includes providing assurances that information and assets are controlled and secured, access is easily available to the masses, and personal information is protected. The September 11 attacks on our nation further underscore the need for governments to protect their information and assets to both preserve citizen trust and prevent disruption of governmental operations through cyber terrorism.

A project team was formed from the NECCC Citizens Trust and Confidence Workgroup to explore governments' use of seal programs to provide assurances to citizens. An analysis of the various seal programs noted that they do not cover all of the areas unique to the government environment. Given this, and the fact that a seal could be in essence a graphical representation of audit results for a government web site, the project team opted to provide an overview of the various levels of branding that governments can do, including the aspects of assurances that a seal program would cover. This document contains narrative and tools to enable both governmental entities and their auditors to review current practices and assure that proper controls are in place for citizen trust and confidence to be achieved.

To facilitate the process of publishing information and providing access to services on the Web, government entities should establish specific policies, procedures, and responsibilities for creating and updating information on its Web site. Key issues to be considered in providing access to government information and services include:

Accessibility and Usability – provides that access to its information, services, and programs are accessible, understandable and navigable.

Privacy and Security – details the information a government Web site collects and how it will be used, under what conditions the information may be shared or released to another party, and the security procedures to ensure that information collected from consumers is accurate and secure from unauthorized use. In some states, privacy will be a challenge as many types of information created by a government entity are largely considered to be in the public domain.

Privacy in the online arena includes disclosing how personal information is collected, used, and shared within a government or between other levels of government, or private entities, and how that information is protected. To achieve this objective, numerous private organizations have designated a Chief Privacy Officer (CPO) to ensure that privacy and security policy and practices are implemented and followed.

This paper will address how a state or a state agency can create an entity responsible for creating, implementing, and overseeing a privacy and security policy for government services and transactions conducted on the Internet.

A new e-Government study of 1,680 state and federal government websites by Brown University, indicated that 28 percent of the states now have some form of privacy policy on their site, up from 7 percent in 2000, and eighteen percent now have a visible security policy, up from 5 percent last year. While this study indicates that state websites are improving, considerable work is necessary if citizens are expected to have trust and confidence in e-Government programs.

The NECCC published "Privacy Policies – Are You Prepared? – A Guidebook for State and Local Government" at its 2000 annual conference. The guidebook recommended the following:

> "Each state and local government should adopt a privacy policy and take responsibility for enforcing it among its divisions and departments. Thoughtful consideration should be given to the parameters for the policy as well as its legal implications before it is posted."

The NECCC guidebook included an assessment tool to allow agencies and auditors to administer an evaluation of the issues relating to the establishment of privacy and accessibility policies. This document expands on that concept and addresses several options available to government organizations. It includes more detailed assessment tools for both government organizations and auditors to use in assessing controls over privacy and accessibility.

II. Validating Government Websites

This section addresses how a citizen can ascertain whether they are dealing with an official electronic-government (e-Gov) web site. The agency must address two fundamental issues: first, the citizen may not know what government agency or level of government provides a specific service; and, second,

whether the information they found on the Internet is from an official government site. Furthermore, because there is no common set of standards that all government sites comply with, the citizen may choose not to conduct on-line transactions because of the potential for privacy or security problems. This problem is further compounded by some government entities establishing e-Gov portals under new web addresses that do not follow the standard www.state.xx.us naming.

Website branding is a statement that the website complies with an established set of practices regarding such issues as the collection, use and disclosure of personally identifiable information collected by the site. Because the branding identifies the specific practices that the branded site subscribes to with respect to such issues as accessibility/usability, privacy and security, the public can have a greater level of trust when using the web site because the website policies must comply with standards established and monitored by a third party.

Branding can be achieved at various levels of integration. In its simplest form branding may only address a common look (e.g., specific image files) and feel (e.g., common links and layout) to the websites. The next type of branding program could use an informal seal, such as a specific image file, to designate compliance with a specified set of policies. Perhaps the most comprehensive form of branding is the use of a seal that provides authentication throughout the group members (e.g., a state). This type of branding program would use a specific image that is required by statute or regulation and could be tied to server certificate and formal registration. A citizen clicking on the image would go to a central site that would confirm that the site was an official government site, the agency operating the site, and could include additional information such as the common standards, policies and practices required by registered sites and audit reports regarding the site. Regardless of the level of branding deployed, an audit, whether internal or external, has a role in verifying that the common policies, practices, and controls are properly implemented and consistently followed.

III. Accessibility

The Americans with Disabilities Act has been interpreted by the US Department of Justice to require covered entities, including state agencies, to ensure that Internet based applications, services, and transactions are accessible as provided in the Act. The World Wide Web Consortium (W3C) has published Web Content Accessibility Guidelines that address a range of standards for text, audio, and video usage on web sites. The Federal Access Board has also published standards for the federal government, under Section 508, that addresses Web-based intranet and Internet information and applications.

An Accessibility Assessment Questionnaire is included as Appendix A.

IV. Privacy and Security

The establishment of a privacy and security policy for agency web based activities involves the application of existing laws regarding freedom of information and/or personal privacy protection to this new medium of receiving and accessing information. Several states either have statutes or executive orders addressing the establishment of privacy policies for agency websites. The more difficult situation, which this paper will address, is how to proceed in the absence of executive or statutory directive. This paper will provide guidelines for establishing a privacy and security policy for agency web sites. A Privacy Assessment Questionnaire is included as Appendix B.

Before we address the substantive issues regarding the creation of a privacy and security policy, we must first identify and articulate the purpose for the policy. Fortunately, this can be done in one word: trust. The first and foremost purpose of the privacy and security policy is to establish and maintain the public's trust in the agency's ability to conduct its activities on the internet without compromising the integrity of the information collected and accessed by the web site. In order for an agency's website to be effective

and productive it is imperative that gaining and maintaining the public's trust be designed into all activities on and relating to the website.

Agency management must recognize the importance of the privacy and security policy and the manner in which the policy impacts all aspects of the web site and the agency's operations. First, agency management must identify the person or persons responsible for establishing, overseeing and updating the privacy and security policy (hereinafter, privacy entity). Second, because the privacy and security policy is the foundation for establishing and maintaining the public's trust in the agency's web site, agency management should establish and acknowledge within the agency a strong relationship with the privacy entity to ensure that the importance of the privacy and security policy is communicated to all agency personnel. Third, because the privacy and security policy applies to all aspects of the agency's web site, agency management should provide that the privacy entity either consult with or be compromised of representatives from the following program areas: legal, security, policy and applications. These steps will ensure that the privacy entity has the tools, resources and authority to address both current privacy issues as well as those that develop in the future.

- The first task for the privacy entity is to catalog the agency's web-based activities and identify the information, if any, collected by each activity. These tasks are ongoing, and must be done for each revision of an existing activity and each new activity added to the agency's web site. Web based activities generally fall into the following categories:
- static information (web browsing); transactions; and e-mail. The information potentially gathered by a web site generally fall into the following categories: personally identifiable information (PII), which is generally defined as information that can personally identify the user such as name, mailing address, telephone number, social security number, and e-mail address;
- non-personally identifiable information, which is generally defined as information the internet enables the operator of a website to collect but that does not personally identify an individual, such as the Internet Protocol address and domain name of the users Internet service provider, the type of browser and operating system employed by the user, the date and time the user visited the agency

website, the web pages or services the user accessed at the agency website, and the URL or web site address of the website the user visited prior to coming to agency website and from which any web page on this site was linked; and,

- sensitive information, which is generally defined as information that is not generally available and that a person would not ordinarily disclose, such as financial or health related information.

The second task for the privacy entity is to identify existing statutory, regulatory, or common law requirements relating to the collection, storage, and disclosure of agency records, regardless of the type of information contained in the records, and assess how the web based applications can satisfy these requirements. The collaboration of the various program areas is necessary to address the challenges presented by the Internet with respect to collecting, storing, and disclosing information. The legal team will identify and evaluate the record retention and disclosure requirements. The policy team must identify the types of the information each web-based activity will collect. The security team must identify the parameters for ensuring the information can be securely collected and stored by the agency, and, if necessary, accessed by the user. The applications team must design an application that incorporates both the data collection requirements and security concerns, as well as being user friendly.

The third task is to determine, based on the number and type of applications, whether one privacy and security policy is sufficient or whether certain applications require a separate and distinct privacy and security policy. Because establishing and maintaining the citizen's trust is the paramount purpose of the privacy and security policy, prominent notice should be provided to the citizen whenever a separate private and security policy is required for an application explaining why the agency's generic privacy and security policy is not sufficient and how the particular privacy and security policy addresses the concerns of the particular application.

The fourth task is to determine whether and how citizens can gain access over the Internet to information they provided in an agency application for the purpose of reviewing and correcting the information. However, before the agency can address the issue of people accessing information they provided to the agency via the Internet, the agency must be able to identify and authenticate the person to ensure they

are the person entitled to the information. The necessity to identify and authenticate a citizen highlights the benefits of a multi-team privacy entity because the policy team will identify the applications requiring these services as well as potentially unique information that can be used in the identification and authentication process, the security team will propose solutions, the legal team will review the proposed solution for compliance with statutory or regulatory requirements, and the applications team will incorporate the identification and authentication process into the application. The final portion of allowing users of the agency website access to information they provided on the website is to establish audit and control functions. The audit and control procedures serve two functions: first, to ensure internal compliance with the privacy and security policy; and, second, to demonstrate to external entity's compliance with the privacy and security policy.

Trust must be earned each time a person accesses an agency website. Accordingly, the privacy and security policy is not a static document, but a constant work in progress, ever changing to address both changes in the nature and manner the agency delivers services and transactions via the internet, as well as any additional record retention or disclosure requirements. Therefore, continued support of agency management for the privacy entity is essential for maintaining citizen trust in the agency's web applications. Incorporating persons from the various agency program teams ensures that the privacy entity can address the diversity of issues that will impact the privacy and security policy as the internet becomes a more common means of providing citizens and businesses better access to government services. For these reasons, the privacy entity should continue to exist beyond the drafting of the privacy and security policy to address, proactively, any issues relating to the privacy and security policy.

With the dependence that government agencies place on their electronic information systems, and the proliferation of non-secured networks, such as the internet, adequate security is essential to citizen confidence and trust. In December 2000, the NECCC published a "Risk Assessment Guide to e-Commerce/e-Government". The guide lays out the risks agencies face where security is concerned.

In determining which technology is appropriate for a given transaction the agency must include a risk assessment and an evaluation of targeted customer or user needs. The initial use of the risk assessment is to identify and mitigate risks in the context of available technologies and their relative total costs and effects on the program being analyzed. The assessment should also be used to develop baselines for verifiable performance measures that track the agency's mission, strategic plans, and performance objectives. While recognizing that achieving absolute security for any application is difficult and expensive, agencies must strike a balance between the security of the application and the usability of the application.

A vital part of both creating citizen trust in government web sites and making transactions on such web sites secure is establishing strong identity and authentication protocols of persons undertaking transactions on such sites. If authentication is required, several options are available: ID and Passwords for a web-based transaction may be sufficient, however the user login session should be encrypted using Secure Sockets Layer (SSL) to protect the transmission of sensitive data.

Encryption is a crucial element of protecting information on the Internet. There are a variety of levels of encryption and the level of encryption used depends on both the sensitivity of the information and the method by which the information is being exchanged. Filing a form through a web site may not require security, however, if the form requests any personally identifiable information, or the user is accessing a specific application that requires a user ID and password, then the session (transmission) should be encrypted. The most common form of securing this type of transmission is Secure Sockets Layer (SSL), a protocol for server authentication (verifying the server's identity to the client), thereby ensuring the citizen that they are communicating with the agencies server. . Employing SSL is a crucial link in establishing and maintaining citizen trust and confidence in government Internet services and transactions.

The National State Auditor’s Association and the General Accounting Office are currently working on a framework to establish or enhance a security audit function, including a guide, toolsets and training. This work covers not only security at a particular governmental location or for a program, but also where the

boundaries cross, and systems interact with other government entities and the private sector. Due to this ongoing project, the project team chose to not include tools for reviewing security, deferring this to the upcoming results of this other project.

Model Privacy and Security Policy

Introductory language.

The policy should identify the scope of agency applications to which the policy applies and provide an overview about the agency's privacy practices.

Example: The Department of X maintains this site as a public service. The following is the privacy and security policy for this site (all pages starting with www.XXX.state.xx.us):

Information collected and stored automatically.

In the course of operating a web site certain information may be collected automatically by such means as logs or by cookies. These sources may allow an agency to collect a great deal of information, however, the agency as a policy matter may elect only to collect limited information. The privacy and security policy should make clear what information the agency is collecting this type of information and whether it will take further steps to collect more information.

Example: We do not use cookies to collect information.

Notes: A cookie file contains unique information a web site can use to track such things as passwords, lists of pages you've visited, and the date when you last looked at a specific page or to identify your session at a particular web site. A cookie is often used in commercial sites to identify the items selected for a specific shopping cart application.

Cookies come in several types, primarily session or persistent. They may be set and controlled, by the site itself or another site, a third-party in a different domain. Agencies that are providing access to information and services may have a valid requirement to use session cookies, providing that the use is disclosed in the associated privacy and security policy. A new technology called a Web bug is being used by some web sites to track and/or report information about a visitor to a web page. Web bugs are also called Web Beacons or Clear GIFs. In order for visitors to make informed decisions about the privacy practices of state agencies, the visitor should be able to access the home page and Privacy and Security Policy page without the site setting a cookie or using a web bug to track the visitor.

Example: For site management functions, information is collected for analysis and statistical purposes. This information is not reported or used in any manner that would reveal personally identifiable information, and will not be released to any outside parties unless legally required to do so in connection with law enforcement investigations or other legal proceedings.

Example: We use Log analysis tools to create summary statistics, which are used for purposes such as assessing what information is of most interest, determining technical design specifications, and identifying system performance or problem areas. The following information is collected for this analysis:

User Client hostname - The hostname (or IP address if DNS is disabled) of the user/client requesting access.

HTTP header, "user-agent" - The user-agent information includes the type of browser, its version, and the operating system it's running on.

HTTP header, "referrer" - The referrer specifies the page from which the client accessed the current page.

System date - The date and time of the user/client request.

Full request - The exact request the user/client made.

Status - The status code the server returned to the user/client.

Content length - The content length, in bytes, of the document sent to the user/client.

Method - The request method used.

Universal Resource Identifier (URI) - The location of a resource on the server.

Query string of the URI - Anything after the question mark in a URI.

Protocol - The transport protocol and version used.

Note: If the site uses cookies, the policy should identify what information is collected and how that information is used and protected.

Information Collected from E-mails and Web Forms.

Many websites receive personally identifiable information from e-mails or web forms. The privacy and security policy should state how the personally identifiable information in these mediums is treated.

Example: If you send us an electronic mail message with a question or comment that contains personally identifying information, or fill out a form that e-mails us this information, we will only use the personally-identifiable information to respond to your request and analyze trends. We may redirect your message to

another government agency that is in a better position to answer your question. We will not sell or release your e-mail address unless you affirmatively consent to the sale or release of the information.

Security, Intrusion, Detection Language.

Many agency sites use information collected on a site to detect potentially harmful intrusions and to take action once an intrusion is detected. The agency's policy may be not to collect personally identifiable information from such sources as IP logs, provided, however, in the event of an intrusion as part of the authorized law enforcement investigations, and pursuant to any required legal process, information from those logs and other sources may be used to help identify the individual that committed the intrusion.

Example: For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with _____.

Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the _____ Penal Code Chapters XX and ZZ.

V. Audit and Public Reporting

An important tool in building and maintaining the public's trust and confidence is to utilize the governmental entity's independent auditor for reviewing branding mechanisms, including the adherence to the privacy and security policy's procedure for securing and disclosing personally identifiable

information. Their public reporting mechanisms should give citizens confidence in their work, and in government's openness to exposing and correcting privacy and security issues. However, parameters must be established to provide that information gained through their audit process, such as security vulnerability reports and personally identifiable information, are not contained in a final report. To that end, several states have already introduced or passed legislation to keep security vulnerability reports that contain information that could compromise the security of state systems exempt from public disclosure. For example, the Texas State legislature recently passed House bill 249, which can be found at http://www.capitol.state.tx.us/tlo/77R/billtext/HB00249F.HTM

VI. Conclusion

The creation of a branding mechanism, seal program or of a privacy and security policy, either individually or collectively, serves the same purpose; to establish and maintain the public's trust in the government's ability to provide services and transactions via the Internet in a manner that preserves the integrity, and where appropriate, the confidentiality of the information. The complex issue involved in placing government services and transactions on the Internet is not the technology, but rather, in developing, implementing and monitoring the policy and procedures behind the technology. In the aftermath of September 11 and the conflict the United States is now engaged in heightens the need to protect government information.

The branding procedures recommended by this Paper, the assessment tool and the guide to establishing a privacy entity, are intended to enable an agency to conduct an examination of its information procedures; evaluate them; continue them where appropriate; but, most importantly, to rescind those policies that do not support the agencies ability to provide services and transactions on the Internet, and to create policies that further this objective. With respect to branding, because it is an enterprise solution, each state or agency must determine the level and type of branding that is appropriate for its circumstances.

Both the privacy and security policy and the branding program are designed to convince the public that it can have confidence in the government's ability to provide services and transactions via the Internet in a secure and reliable manner. In preparing to offer Internet based services it is crucial to remember that their use by the public is entirely at the public's discretion. Failure to comprehend this fact and the policy issues associated with this undertaking could defeat all efforts to establish the Internet as a viable, if not more desirable alternative to the paper based world for conducting business with the government. The public will not leave the in-line world for the online world unless the government can convince the public that it can trust the government's ability to collect and protect their information in this new medium.

VII. Appendices

Appendix A

Accessibility Assessment Questionnaire

1. Do web pages have a text equivalent for every non-text element (e.g., via "alt", "longdesc", or in element content)?

2. Do multimedia presentations have equivalent alternatives synchronized with the presentation?

3. Are web pages designed so that all information conveyed with color is also available without color?

4. Are documents organized so they are readable without requiring an associated style sheet?

5. Are redundant text links provided for each active region of a server-side image map?

6. Are client-side image maps provided instead of server-side image maps except where the regions cannot be defined with an

available geometric shape?

7. Are row and column headers identified for data tables?

8. Do tables use markup to associate data cells and header cells for data tables that have two or more logical levels of row or

column headers?

9. If frames are used, are they titled with text that facilitates frame identification and navigation?

10. Are web pages designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz?

11. Is a text-only page, with equivalent information or functionality, provided to make a website accessible, when compliance cannot

be accomplished in any other way? Is the content of the text-only page updated whenever the primary page changes?

12. If web pages utilize scripting languages to display content, or to create interface elements, is the

information provided by the script identified with functional text that can be read by assistive technology?

13. If a web page requires that an applet, plug-in or other application be present on the client system to interpret page content, does

the page provide a link to the plug-in or applet?

14. If electronic forms are designed to be completed on-line, does the form allow people using assistive technology to access the

information, field elements, and functionality required for completion and submission of the form, including all directions and cues?

15. Is a method provided that permits users to skip repetitive navigation links?

16. If a timed response is required, is the user alerted and given sufficient time to indicate more time is required?

17. Are web pages designed to work on older versions of browsers?

Appendix B

Privacy Assessment Questionnaire

1. Does the organization have a clearly written privacy and security policy? (If no, skip to question 3)

2. Is the policy prominently posted at all entry points to the web site and on all pages where personally identifiable information is requested or an email can be sent?

3. Does the organization have a Chief Privacy Officer? If not, has a specific employee or department been assigned the responsibility for implementing and monitoring a privacy policy? What is their reporting relationship to the entity's management? (If no, go to #5)

4. Does the entity's web site contain information regarding how to contact this employee or unit with questions regarding privacy and the site?

5. Has the organization taken specific steps to implement the privacy policy? (If no, go to #7) Describe the steps take to implement the privacy policy:

6. (a.) Are all employees aware of the privacy and security policy and the importance of maintaining citizen confidentiality? (b.) Are all employees appropriately trained, on privacy policies of the organization? (c.) If so, is the training based on their level of access to the personally identifiable information the agency collects? (d.) Are new employees made aware of the privacy policy when employed by the organization?

7. (a.) Does the policy cover all web pages operated by the organization? (b.) If not, does the policy disclose the web pages covered by the policy?

8. Does the organization collect personally identifiable information through the web site? (If yes, go to 10)

9. Does the web site explain that it does not collect personally identifiable information? How does the organization control this? (End of Assessment)

10. Does the privacy and security policy disclose the following: (If the organization does not have a privacy policy, you are finished)
    1. The individually identifiable information that is collected and how it is collected?
        a. Does the privacy and security policy specify the types or personally identifiable information that is collected?
        b. Does the privacy and security policy specify the means in which it is collected, i.e. via email, on-line forums, forms, other transactions?
    2. The intended use of and ultimate disposition of the collected data:
        a. Does the privacy and security policy state consequences for failing to provide personally identifiable information?
    3. Whether the information is shared with third parties, who the third parties are, what information is shared, and the purpose for sharing it?
    4. Whether individuals may choose to have their personally identifiable information collected or shared with third parties?
        a. Does the privacy and security policy inform individuals about applicable public records laws that affect their information?
    5. Does the organization provide individuals the choice of opting out of having their personally identifiable information shared? Is the “opt out” option given at the time of collection? Are the “opt in” and “opt out” options clearly stated in the privacy and security policy?
    6. How the organization maintains the security of the personally identifiable information it receives and stores?

a. Does the organization physically control access to the storage devices where this information is stored, including all copies such as back-ups?

b. Does the organization apply appropriate security measures to protect electronic access to this information?

c. Are the above security measures included in the privacy and security policy?

7. How the organization maintains the accuracy of the personally identifiable information it receives and stores?

   a. Are procedures in place to help assure the accuracy of personally identifiable information?

   b. Describe the procedures to help assure the accuracy of personally identifiable information._____

   _____

   _____

8. How individuals may review their information and request corrections if necessary?

   a. Does the privacy and security policy explain the steps an individual can go through to ensure the information collected by the agency is correct?

   b. Describe the steps an individual can go through to ensure their information is correct:_____

   _____

   _____

   c. Do individuals have on-line access to their personally identifiable information collected through the agency's website ?

   Does the organization limit the number of times an individual may access their information, and if so, is this limit specifically stated in the privacy and security policy?

9. Does the organization take necessary steps to authenticate the identity of the individual requesting access to and/or correction to their information?

   a. Describe the steps to authenticate the identity of the individual requesting access to and/or correction to their personally identifiable information collected through the

agency's web site_____

_____

_____

10. How to resolve complaints relating to the accuracy and completeness of an individual's information, and the consequences for failure to resolve such complaints?
11. Any information that is collected involuntarily (by accessing the web site), such as user identification, locations visited on the web site?
    a. Does the privacy and security policy describe how permission is obtained before storing, altering or copying information in the individual's computer or that the individual is notified with an option to prevent such activity?
    b. Does the organization use server logs and for what purpose? Is the use clearly stated in the policy? Are the contents of the server logs disclosable under statute, regulation, or the privacy policy?
    c. Describe the process for authorizing and controlling the use of cookies:___

       _____
    d. Does the web site use session cookies? Are session cookie purged when the user exits the site?
    e. Does the web site use persistent cookies? Is there a process for authorizing the use of persistent cookie?
    f. Does the privacy and security policy describe the consequences for refusing to accept a cookie?

12. How personally identifiable information is merged with data from other sources, and how merged information is used, including who has access to this information?

13. Sensitive information such as social security numbers, credit card numbers, health-care information that is collect through the organization's web site, and how the information is

protected during transmission (such as encryption)? _____ Describe the process for protecting this information during transmission:_____

_____

11. If the web site has a child-specific page, does the policy comply with Children's Online Privacy Protection Act?

12. Does the policy comply with other laws relating to student information, medical information, financial information, or law enforcement?

Appendix C

John J. Aveni

Lawrence F. Alwin, CPA

J. Kenneth Blackwell

Tom Bossie

Ralph Campbell, Jr.

Frank M. Dean

David DeStefano

Christina Dorfhuber

Scott Etter

Bonnie Ettinger

Ed Fraga

Scott Frendt

Danielle Germain

Dan Greenwood

Michele Grisham

Raymond C. Headen

Marc Hiller

Jerry Johnson

Mary Kiffmeyer

Michele Kryszak

Wanda Lairson

Brandon Lenoir

Alia Mendonsa

Kathy Minchew

Bob Moriarty

Basil Nikas

Darby Patterson

Nancy Rainosek

Leslie Reynolds

Matthew Rosenthal

Eric Seabrook

Bill Sullivan

Martin Vernon

Tom Wagner

Karen West

Lynne M. Wolstenholme