EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

December 16, 2003

M-04-04

MEMORANDUM TO THE HEADS OF ALL DEPARTMENTS AND AGENCIES

FROM: Joshua B. Bolten
Director

SUBJECT: E-Authentication Guidance for Federal Agencies

The Administration is committed to reducing the paperwork burden on citizens and businesses, and improving government response time to citizens – from weeks down to minutes. To achieve these goals, citizens need to be able to access government services quickly and easily by using the Internet. This guidance document addresses those Federal government services accomplished using the Internet online, instead of on paper. To make sure that online government services are secure and protect privacy, some type of identity verification or authentication is needed.

The attached guidance updates guidance issued by OMB under the Government Paperwork Elimination Act of 1998, 44 U.S.C. § 3504 and implements section 203 of the E-Government Act, 44 U.S.C. ch. 36. This guidance also reflects activities as a result of the E-Authentication E-Government Initiative and recent standards issued by the National Institute of Standards and Technology (NIST). In preparing this guidance, we have worked closely with and incorporated comments from agency Chief Information Officers.

This guidance takes in account current practices in the area of authentication (or e-authentication) for access to certain electronic transactions and a need for government-wide standards and will assist agencies in determining their authentication needs for electronic transactions. This guidance directs agencies to conduct “e-authentication risk assessments” on electronic transactions to ensure that there is a consistent approach across government. (see Attachment A). It also provides the public with clearly understood criteria for access to Federal government services online. Attachment B summarizes the public comments received on an earlier version of this guidance.

For any questions about this guidance, contact Jeanette Thornton, Policy Analyst, Information Policy and Technology Branch, Office of Management and Budget, phone (202) 395-3562, fax (202) 395-5167, e-mail: eauth@omb.eop.gov.

Attachments
Attachment A – E-Authentication Guidance for Federal Agencies
Attachment B – Summary of Public Comments and Responses

Attachment A

E-Authentication Guidance for Federal Agencies

1. Introduction

1.1. Summary

This guidance requires agencies to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance. It establishes and describes four levels of identity assurance for electronic transactions requiring authentication. Assurance levels also provide a basis for assessing Credential Service Providers (CSPs) on behalf of Federal agencies. This document will assist agencies in determining their e-government authentication needs. Agency business-process owners bear the primary responsibility to identify assurance levels and strategies for providing them. This responsibility extends to electronic authentication systems.

Agencies should determine assurance levels using the following steps, described in Section 2.3:

1. Conduct a risk assessment of the e-government system.
2. Map identified risks to the applicable assurance level.
3. Select technology based on e-authentication technical guidance.
4. Validate that the implemented system has achieved the required assurance level.
5. Periodically reassess the system to determine technology refresh requirements.

1.2. Scope

- This guidance applies to remote authentication of human users of Federal agency IT systems for the purposes of conducting government business electronically (or e-government). Though that authentication typically involves a computer or other electronic device, this guidance does not apply to the authentication of servers, or other machines and network components.
- This guidance is intended to help agencies identify and analyze the risks associated with each step of the authentication process. The process includes (but is not limited to) identity proofing, credentialing, technical and administrative management, record keeping, auditing, and use of the credential. Each step of the process influences the technology's overall conformance to the desired assurance level.

- This guidance supplements OMB Circular A-130, Management of Federal Information Resources, Appendix II, Implementation of the Government Paperwork Elimination Act (GPEA).
- This guidance does not directly apply to *authorization*. Authorization focuses on the actions *permitted* of an identity after authentication has taken place. Decisions concerning authorization are and should remain the purview of the business process owner.
- This guidance does not address issues associated with "intent to sign," or agency use of authentication credentials as electronic signatures. For more information on electronic signatures, see the OMB guidance on implementing GPEA[1] and the Electronic Signatures in Global and National Commerce Act, Pub. L. No. 106-229[2].
- This guidance does not identify which technologies should be implemented. The Department of Commerce's National Institute for Standards and Technology (NIST) is developing complementary e-authentication technical guidance that agencies will use to identify appropriate technologies, based on the analysis process described here.
- This document does not confer, and may not be used to support, any right on behalf of any person or entity against the United States or its agencies or officials.

1.3. Overview

This document provides agencies with guidance on electronic authentication (e-authentication). The National Research Council report, "Who Goes There? Authentication Through the Lens of Privacy"[3] defines e-authentication as the process of establishing confidence in user identities electronically presented to an information system. It defines individual authentication as the process of establishing an understood level of confidence that an identifier refers to a specific individual.

Authentication focuses on confirming a person's identity, based on the reliability of his or her credential. *Authorization* focuses on identifying the person's user permissions.

To successfully implement a government service electronically (or e-government), Federal agencies must determine the required level of assurance in the authentication for each transaction. This is accomplished through a risk assessment for each transaction. The assessment identifies:

a) risks, and

b) their likelihood of occurrence.

OMB Circular A-130, Management of Federal Information Resources, states that agencies must prepare and update a strategy that identifies and mitigates risks associated with each information system. This guidance will help agencies map identified risks to corresponding assurance levels.

---

1 OMB Memorandum M-00-10, 4/25/00, http://www.whitehouse.gov/omb/memoranda/m00-10.html

2 OMB Memorandum M-00-15, 9/25/00, http://www.whitehouse.gov/omb/memoranda/m00-15.html

3 March 31, 2003, http://www.nap.edu/books/0309088968/html/

Section 5 of the GPEA guidance details the risk factors agencies should consider in planning and implementing e-government transactions and systems. This document expands on Section 5 by instructing agencies how to implement e-authentication processes by

- outlining a process for assessing risk,
- describing four levels of identity assurance, and
- explaining how to determine the appropriate level of identity assurance.

1.4. Applicability

Not all Federal electronic transactions[4] require authentication; however, this guidance applies to all such transactions for which authentication *is* required, regardless of the constituency (e.g. individual user, business, or government entity).

Transactions not covered by this guidance include those that are associated with national security systems as defined in 44 U.S.C. § 3542(b)(2). Private-sector organizations and state, local, and tribal governments whose electronic processes require varying levels of assurance may consider the use of these standards where appropriate.

There are two types of individual authentication:

a) Identity authentication—confirming a person's unique identity.

b) Attribute authentication—confirming that the person belongs to a particular group (such as military veterans or U.S. citizens).

Attribute authentication is the process of establishing an understood level of confidence that an individual possesses a specific attribute. If the attribute does not provide ties to the user's identity; it would be considered an *anonymous credential* (discussed further in Section 4.2). Attribute authentication is not specifically addressed in this document, however agencies may accept 'anonymous credentials' in certain contexts.

2. Assurance Levels and Risk Assessments

2.1. Description of Assurance Levels

This guidance describes four identity authentication assurance levels for e-government transactions. Each assurance level describes the agency's degree of certainty that the user has presented an identifier (a credential[5] in this context) that refers to his or her identity. In this context, assurance is defined as 1) the degree of confidence in the *vetting process* used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

The four assurance levels are:

---

4 For the purposes of this document, a transaction is defined as: a discrete event between user and systems that supports a business or programmatic purpose.

5 A credential is defined as: an object that is verified when presented to the verifier in an authentication transaction.

- Level 1: Little or no confidence in the asserted identity's validity.
- Level 2: Some confidence in the asserted identity's validity.
- Level 3: High confidence in the asserted identity's validity.
- Level 4: Very high confidence in the asserted identity's validity.

2.2. Risks, Potential Impacts, and Assurance Levels

While, this guidance addresses only those risks associated with authentication errors, NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems," recommends a general methodology for managing risk in Federal information systems. In addition, other means of risk management, (e.g., network access restrictions, intrusion detection, and event monitoring) may help reduce the need for higher levels of authentication assurance.

Potential Impact Categories: To determine the appropriate level of assurance in the user's asserted identity, agencies must assess the potential risks, and identify measures to minimize their impact. Authentication errors with potentially worse consequences require higher levels of assurance. Business process, policy, and technology may help reduce risk. The risk from an authentication error is a function of two factors:

a) potential harm or impact, and

b) the *likelihood* of such harm or impact.

Categories of harm and impact include:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss or agency liability
- Harm to agency programs or public interests
- Unauthorized release of sensitive information
- Personal safety
- Civil or criminal violations.

Required assurance levels for electronic transactions are determined by assessing the potential impact of each of the above categories using the potential impact values described in Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems." The three potential impact values are:[6]

- Low impact
- Moderate impact
- High impact.

---

6 For the purposes of this document, the impact value *not applicable* may apply to the categories of harm.

The next section defines the potential impacts for each category. Note: If authentication errors cause no measurable consequences for a category, there is "no" impact.

Determining Potential Impact of Authentication Errors:

Potential impact of ***inconvenience, distress, or damage to standing or reputation***:

- **Low—**at worst, limited, short-term inconvenience, distress or embarrassment to any party.
- **Moderate—**at worst, serious short term or limited long-term inconvenience, distress or damage to the standing or reputation of any party.
- **High—**severe or serious long-term inconvenience, distress or damage to the standing or reputation of any party (ordinarily reserved for situations with particularly severe effects or which affect many individuals).

Potential impact of ***financial*** *loss*:

- **Low—**at worst, an insignificant or inconsequential unrecoverable financial loss to any party, or at worst, an insignificant or inconsequential agency liability.
- **Moderate—**at worst, a serious unrecoverable financial loss to any party, or a serious agency liability.
- **High—**severe or catastrophic unrecoverable financial loss to any party; or severe or catastrophic agency liability.

Potential impact of ***harm to agency programs or public interests***:

- **Low—**at worst, a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with *noticeably* reduced effectiveness, or (ii) minor damage to organizational assets or public interests.
- **Moderate—**at worst, a serious adverse effect on organizational operations or assets, or public interests. Examples of serious adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with *significantly* reduced effectiveness; or (ii) significant damage to organizational assets or public interests.
- **High—**a severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (i) severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interests.

Potential impact of ***unauthorized release of sensitive information***:

- **Low—**at worst, a limited release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact as defined in FIPS PUB 199.
- **Moderate—**at worst, a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a moderate impact as defined in FIPS PUB 199.

- **High—**a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a high impact as defined in FIPS PUB 199.

Potential impact to ***personal safety***:

- **Low—**at worst, minor injury not requiring medical treatment.
- **Moderate—**at worst, moderate risk of minor injury or limited risk of injury requiring medical treatment.
- **High—**a risk of serious injury or death.

The potential impact of ***civil or criminal violations*** is:

- **Low—**at worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts.
- **Moderate—**at worst, a risk of civil or criminal violations that may be subject to enforcement efforts.
- **High—**a risk of civil or criminal violations that are of special importance to enforcement programs.

Determining Assurance Level:

Compare the impact profile from the risk assessment to the impact profiles associated with each assurance level, as shown in Table 1 below. To determine the required assurance level, find the lowest level whose impact profile meets or exceeds the potential impact for every category analyzed in the risk assessment (as noted in step 2 below).

Table 1 – Maximum Potential Impacts for Each Assurance Level

	Assurance Level Impact Profiles			
Potential Impact Categories for Authentication Errors	**1**	**2**	**3**	**4**
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

In analyzing potential risks, the agency must consider all of the potential direct and indirect results of an authentication failure, including the possibility that there will be more than one failure, or harms to more than one person. The definitions of potential impacts contain some relative terms, like "serious" or "minor," whose meaning will depend on context. The agency should consider the context and the nature of the persons or entities affected to decide the relative significance of these harms. Over time, the meaning of these terms will become more definite as agencies gain practical experience with these issues. The analysis of harms

to agency programs or other public interests depends strongly on the context; the agency should consider these issues with care.

In some cases (as shown in Table 1), impact may correspond to multiple assurance levels. For example, Table 1 shows that a moderate risk of financial loss corresponds to assurance levels 2 and 3. In such cases, agencies should use the context to determine the appropriate assurance level.

2.3. Determining Assurance Levels and selecting authentication solutions using Risk Assessment

Agencies shall use the following steps to determine the appropriate assurance level:

Step 1: Conduct a risk assessment of the e-government system. Guidance for agencies in conducting risk assessments is available in A-130, Section 5 of OMB's GPEA guidance and existing NIST guidance. The risk assessment will measure the relative severity of the potential harm and likelihood of occurrence of a wide range of impacts (to any party) associated with the e-government system in the event of an identity authentication error.

Note: An E-government system may have multiple categories or types of transactions, which may require separate analysis within the overall risk assessment. An E-government system may also span multiple agencies whose activities may require separate consideration.

Risk analysis is to some extent a subjective process, in which agencies must consider harms that might result from, among other causes, technical failures, malevolent third parties, public misunderstandings, and human error. Agencies should consider a wide range of possible scenarios in seeking to determine what potential harms are associated with their business process. It is better to be over-inclusive than under-inclusive in conducting this analysis. Once risks have been identified, there may also be ways to adjust the business process to mitigate particular risks by reducing the likelihood that they will occur (see Step 4).

Step 2: Map identified risks to the required assurance level. The risk assessment should be summarized in terms of the potential impact categories in Section 2.2.

To determine the required assurance level, agencies should initially identify risks inherent in the transaction process, regardless of its authentication technology. Agencies should then tie the potential impact category outcomes to the authentication level, choosing the lowest level of authentication that will cover all of potential impacts identified. Thus, if five categories of potential impact are appropriate for Level 1, and one category of potential impact is appropriate for Level 2, the transaction would require a Level 2 authentication. For example, if the misuse of a user's electronic identity/credentials during a medical procedure presents a risk of serious injury or death, map to the risk profile identified under Level 4, even if other consequences are minimal.

Step 3: Select technology based on the NIST e-authentication technical guidance. After determining the assurance level, the agency should refer to the NIST e-authentication

technical guidance to identify and implement the appropriate technical requirements.

Step 4: After implementation, validate that the information system has operationally achieved the required assurance level. Because some implementations may create or compound particular risks, conduct a final validation to confirm that the system achieves the required assurance level for the user-to-agency process. The agency should validate that the authentication process satisfies the systems's authentication requirements as part of required security procedures (e.g., certification and accreditation).

Step 5: Periodically reassess the information system to determine technology refresh requirements. The agency must periodically reassess the information system to ensure that the identity authentication requirements continue to be valid as a result of technology changes or changes to the agency's business processes. Annual information security assessment requirements provide an excellent opportunity for this. Agencies may adjust the identity credential's level of assurance using additional risk mitigation measures. Easing identity credential assurance level requirements may increase the size of the enabled customer pool, but agencies must ensure that this does not corrupt the system's choice of the appropriate assurance level.

2.4. Assurance Levels and Risk Profiles: Descriptions and Examples

Level 1—Little or no confidence exists in the asserted identity. For example, Level 1 credentials allow people to bookmark items on a web page for future reference.

Examples:

- In some instances, the submission of forms by individuals in an electronic transaction will be a Level 1 transaction: (i) when all information is flowing to the Federal organization from the individual, (ii) there is no release of information in return, and (iii) the criteria for higher assurance levels are not triggered. For example, if an individual applies to a Federal agency for an annual park visitor's permit (and the financial aspects of the transaction are handled by a separate contractor and thus analyzed as a separate transaction, the transaction with the Federal agency would otherwise present minimal risks and could be treated as Level 1.

- A user presents a self-registered user ID or password to the U.S. Department of Education web page, which allows the user to create a customized "My.ED.gov" page. A third party gaining unauthorized access to the ID or password might infer personal or business information about the individual based upon the customization, but absent a high degree of customization however, these risks are probably very minimal.

- A user participates in an online discussion on the whitehouse.gov website, which does not request identifying information beyond name and location. Assuming the forum does not address sensitive or private information, there are no obvious inherent risks.

Level 2**—***On balance, confidence exists that the asserted identity is accurate. Level 2 credentials are appropriate for a wide range of business with the public where agencies require an initial identity assertion (the details of which are verified independently prior to any Federal action).*

Examples:

- A user subscribes to the Gov Online Learning Center (www.golearn.gov). The site's training service must authenticate the person to present the appropriate course material, assign grades, or demonstrate that the user has satisfied compensation-or promotion-related training requirements. The only risk associated with this transaction is a third party gaining access to grading information, thereby harming the student's privacy or reputation. If the agency determines that such harm is minor, the transaction is Level 2.

- A beneficiary changes her address of record through the Social Security web site. The site needs authentication to ensure that the entitled person's address is changed. This transaction involves a low risk of inconvenience. Since official notices regarding payment amounts, account status, and records of changes are sent to the beneficiary's address of record, it entails moderate risk of unauthorized release of personally sensitive data. The agency determines that the risk of unauthorized release merits Assurance Level 2 authentication.

- An agency program client updates bank account, program eligibility, or payment information. Loss or delay would significantly impact him or her. Errors of this sort might delay payment to the user, but would not normally result in permanent loss. The potential individual financial impact to the agency is low, but the possible aggregate is moderate.

- An agency employee has access to potentially sensitive personal client information. She authenticates individually to the system at Level 2, but technical controls (such as a virtual private network) limit system access to the system to the agency premises. Access to the premises is controlled, and the system logs her access instances. In a less constrained environment, her access to personal sensitive information would create *moderate* potential impact for unauthorized release, but the system's security measures reduce the overall risk to *low*.

Level 3—***Level 3 is appropriate for transactions needing high confidence in the asserted identity's accuracy. People may use Level 3 credentials to access restricted web services without the need for additional identity assertion controls.***

Examples:

- A patent attorney electronically submits confidential patent information to the US Patent and Trademark Office. Improper disclosure would give competitors a competitive advantage.

- A supplier maintains an account with a General Services Administration Contracting Officer for a large government procurement. The potential financial loss is significant, but not severe or catastrophic, so Level 4 is not appropriate.

- A First Responder accesses a disaster management reporting website to report an incident, share operational information, and coordinate response activities.

- An agency employee or contractor uses a remote system giving him access to potentially sensitive personal client information. He works in a restricted-access Federal office building. This limits physical access to his computer, but system transactions occur over the Internet. The sensitive personal information available to him creates a moderate potential impact for unauthorized release.

Level 4—*Level 4 is appropriate for transactions needing very high confidence in the asserted identity's accuracy. Users may present Level 4 credentials to assert identity and gain access to highly restricted web resources, without the need for further identity assertion controls.*

Examples:

- A law enforcement official accesses a law enforcement database containing criminal records. Unauthorized access could raise privacy issues and/or compromise investigations.

- A Department of Veteran's Affairs pharmacist dispenses a controlled drug. She would need full assurance that a qualified doctor prescribed it. She is criminally liable for any failure to validate the prescription and dispense the correct drug in the prescribed amount.

- An agency investigator uses a remote system giving her access to potentially sensitive personal client information. Using her laptop at client worksites, personal residences, and businesses, she accesses information over the Internet via various connections. The sensitive personal information she can access creates only a moderate potential impact for unauthorized release, but her laptop's vulnerability and her non-secure Internet access raise the overall risk.

2.5. Scope and Elements of Risk

When determining assurance levels, one element of the necessary risk assessment is the risk of denial (or repudiation) of electronically transmitted information. Section 9c of OMB's GPEA guidance states agencies should plan how to minimize this risk by ensuring user approval of such information. Section 8c of the OMB Procedures and Guidance on Implementing GPEA includes guidance on minimizing the likelihood of repudiation.

OMB's GPEA guidance states that properly implemented technologies can offer degrees of confidence in authenticating identity that are greater than a handwritten signature can offer. Conversely, electronic transactions may increase the risk and harm (and complicate redress) associated with criminal and civil violations. The Department of Justice's "Guide for Federal Agencies on Implementing Electronic Processes"[7] discusses the legal issues surrounding electronic government. Legal and enforcement needs may affect the design of an e-authentication system and may also entail generation and maintenance of certain system management documentation.

Legal issues can present significant policy challenges for agencies. Agencies should consider these issues when assigning transactions to assurance levels. Risk assessments should include the potential effects of illegal activities and process failures with respect to:

- agency enforcement priorities
- agency programmatic interests
- broader public interests such as national security, the environment, and economic markets.

Some of these harms (e.g., financial loss or release of personal information) are described in each assurance level; others depend on the agency's programmatic interests. The risk analysis process is necessarily highly contextual, and agencies should consider whether their systems present any distinctive risks.

The risk analysis incorporates this by discussing the risks associated with criminal and civil violations, and harm to agency programs or the public interest. Agencies should remember to consult appropriately with their counsel's office in their determination of this impact. When assessing this risk and designing a process, agencies should consider single acts and patterns of action that could affect agency programs. For example, if sensitive information is available from an agency website, the agency should consider the effects of single acts and possible patterns of such activity when assessing risk levels. (18 U.S.C. 1029, 1030)

Agencies may also decrease reliance on identity credentials through increased risk-mitigation controls. For example, an agency business process rated for Level 3 identity assertion assurance may lower its profile to accept Level 2 credentials by increasing system controls or 'second level authentication' activities. (See Section 2.3, Step 5)

Agencies are expected to follow all relevant guidance issued by the National Achieves and Records Administration (NARA) regarding the handling of electronic records. This guidance

7 http://www.usdoj.gov/criminal/cybercrime/eprocess.pdf

addresses implementation issues further in section 4.1.

3. Assessing Confidence in Credential Service Providers

Since identity credentials are used to represent one's identity in electronic transactions, it is important to assess the level of confidence in the credential. Credential Service Providers (CSPs) are governmental and non-governmental organizations that issue and sometimes maintain electronic credentials. These organizations must have completed a formal assessment against the assurance levels described in this guidance.

The CSP's issuance and maintenance policy influences its e-authentication process trustworthiness. The E-Authentication Initiative will therefore develop an assessment process for the government to determine the maximum assurance level merited by the CSP. For example, if a CSP follows all process/technology requirements for assurance Level 3, a user may use a credential provided by the CSP to authenticate himself for a transaction requiring assurance Levels 1, 2, or 3.

4. Implementing an Authentication Process

4.1. The E-Authentication Process

Each step of the authentication process influences the assurance level chosen. From identity proofing, to issuing credentials, to using the credential in a well-managed secure application, to record keeping and auditing—the step providing the lowest assurance level may compromise the others. Each step in the process should be as strong and robust as the others. Agencies will achieve the highest level of identity assurance through strong identity proofing, a strong credential, and robust management (including a strong archive and audit process). However, the best authentication systems result from well-engineered and tested user and agency software applications. A process currently being developed for enabling authentication across Federal agencies will be published for implementation when complete.

To determine the level of credential required to validate a user's identity, an agency must understand how its business applications process the credential. The agency must identify the requirements for each step in the e-authentication (and *authorization*) process. This includes the following steps:

- Initial enrollment
- Subsequent visits to agency application
- Verification of identity credential
- Transaction management
- Long term records management
- Periodic system tests
- Suspension, revocation, re-issuance

- Audit.

Each step is explained in the e-authentication technical guidance. Responsibility for these steps lies with the business process owner, designated agency, or cross-agency authority.

4.2. Using Anonymous Credentials

Unlike identity authentication, anonymous credentials may be appropriate to use to evaluate an attribute when authentication need not be associated with a known personal identity. To protect privacy, it is important to balance the need to know who is communicating with the Government against the user's right to privacy. This includes using information only in the manner in which individuals have been assured it will be used. It may be desirable to preserve anonymity in some cases, and it may be sufficient to authenticate that:

- The user is a member of a group; and/or
- The user is the same person who supplied or created information in the first place; and/or
- A user is entitled to use a particular pseudonym.

These anonymous credentials have limited application and are to be implemented on a case-by-case basis. Some people may have anonymous and identity credentials. As general matter, anonymous credentials are appropriate for Levels 1 and 2 only.

4.3. Information Sharing and the Privacy Act

When developing authentication processes, agencies must satisfy the requirements for managing security in the collection and storage of information associated with validating user identities. The E-Government Act of 2002, section 208 requires agencies to conduct privacy impact assessments for electronic information systems and collections. This includes performing an assessment when authentication technology is added to an electronic information system accessed by members of the public. For additional information on privacy impact assessments, consult OMB guidance.[8]

Most e-authentication processes capture the following information:

- Information regarding the individuals/ businesses/governments using the E-Gov service
- Electronic user credentials (i.e., some combination of public key certificates, user identifiers, passwords, and Personal Identification Numbers)
- Transaction information associated with user authentication, including credential validation method
- Audit Log/Security information.

To the extent that the authentication process captures information that is protected by the

8 OMB Memorandum M-03-22, http://www.whitehouse.gov/omb/memoranda/m03-22.html

Privacy Act (because it is information about an individual that the agency retrieves by an individual's name or other identifier and thus is maintained in an agency Privacy Act system of records), the agency needs to comply with the Privacy Act with respect to such information.

Authentication data must be protected from unauthorized disclosure or modification. The Privacy Act generally requires that registered users be allowed to have access to and request amendment to information about them maintained in a system of records. Information from the system of records should not be shared, except in accordance with the Privacy Act and other applicable laws.

4.4. Cost/Benefit Considerations

Like any capital purchase, implementing e-authentication requires consideration of the benefit and costs, and thus a cost-benefit analysis is required by the Capital Programming Guide.[9] It is also important to match the required level of assurance against the cost and burden of the business, policy, and technical requirements of the chosen solution.

Benefits typically include:

- increased speed of the transaction
- increased partner participation and customer satisfaction
- improved record keeping efficiency and data analysis opportunities
- increased employee productivity and improved quality of the final product
- greater information benefits to the public
- improved security
- extensive security for highly sensitive information

Costs typically include:

- initial capitalization for application design
- technology acquisition
- testing
- deployment of the functional implementation
- long-term maintenance.

In some cases initial capital cost may be small, with higher long-term maintenance cost. It is therefore important to assess the costs over the life cycle of the system. Authentication errors can result in significant costs to agencies and the public. These costs will be identified by the risk analysis set forth in section 2, and should be included in any cost/benefit analysis.

---

9 OMB Circular A-11, Supplement, http://www.whitehouse.gov/omb/circulars/a11/cpgtoc.html

Burden consists of the following two factors:

a) Costs imposed on non-federal entities

b) Any time demands not captured by the cost estimate, but imposed on the entities by the technical solution.

Overly burdensome systems may affect non-federal entities' use of the system diminishing anticipated benefits and lowering return on investment. If a technical solution for an assurance level is too costly or burdensome, agencies should consider reducing the required assurance level and implementing management controls or business process adjustments to achieve the same level of assurance. If the cost cannot be reduced to an acceptable level through such risk mitigation approaches, then the agency may need to reconsider its vision for the e-authentication system.

Higher assurance levels may require more costly credentials. Minimizing the number of credentials can reduce costs. Refer to Section 3 of the GPEA guidance for additional information on assessing risks, costs, and benefits. The e-authentication technical guidance will provide alternatives for addressing assurance levels, which may help agencies to better manage authentication costs.

5. Effective Dates of Guidance

Agencies must categorize all existing transactions/systems requiring user authentication into one of the described assurance levels by September 15, 2005. Agencies should accomplish this in the following order:

- Systems classified as "major" must be completed by December 15, 2004.
- New authentication systems should begin to be categorized, as part of the system design, within 90 days of the completion of the final E-Authentication Technical Guidance issued by NIST.

The chosen assurance level must be made publicly available through the agency website, the Federal Register, or other means (e.g., upon request). Agency application assurance levels will be posted at a central location for public access by the E-Authentication Initiative.

Beginning in 2004, agencies will be asked to report on their progress in implementing this guidance in their annual E-Government Act Reports to OMB required by section 202(g) of the E-Government Act.

Attachment B

Summary of Public Comments and Responses

On July 11, 2003, in a Federal Register notice [68 FR 41370], the General Services Administration, in coordination with the Office of Management and Budget, published a Draft E-Authentication Policy for Federal Agencies.

We received 47 comments representing Federal agencies, technology vendors and other organizations on the proposed guidance. We considered all comments in developing this final OMB guidance. Comments on the guidance supported establishing the requirement for agencies to follow government-wide e-authentication guidance when implementing electronic transactions and to conduct risk assessments. The following paragraphs summarize the general groupings of comments and our responses.

Comments and Responses

Comments fell into three categories: 1. General comments about the need for, cost of, and philosophies of authentication guidance; 2. Comments specific to sections of the document; and 3. Editorial and stylistic comments. Overall, approximately one third of the submitted comments were adopted, resulting in significant revision and reorganization.

Over half of the comments pertained to the Section 2, Assurance Levels and Risk Assessments, and focused on requests for clarification of the guidance. While the entire guidance was extensively revised, the most extensive revision was in this section. The revisions included improving the assurance level descriptions and eliminating the vague naming convention, clarifying how to determine the appropriate assurance level, as well as the potential impacts of authentication errors, and ensuring accuracy of the examples. The scope and applicability sections were improved, confusing terminology was defined and the guidance was reviewed for greater consistency. The guidance was also changed to more closely align with the recently issued NIST standards (the Federal Information Processing Standard (FIPS) 199) and applicable laws. The guidance was also revised for legal accuracy.