GENERAL SERVICES ADMINISTRATION

[2003–N02]

E-Authentication Policy for Federal Agencies; Request for Comments

AGENCY: Office of Electronic Government and Technology, GSA.

ACTION: Notice of policy and request for comments.

SUMMARY: The General Services Administration, in coordination with the Office of Management and Budget (OMB) request comments on the attached draft policy on E-Authentication for Federal Agencies. GSA has coordinated this draft policy with OMB and will work closely with OMB in reviewing comments and issuing the final policy. In this draft policy, GSA is requiring that agencies implement this E-Authentication Policy, which establishes four assurance levels to create a Governmentwide standard framework for determining what is required to access a particular Government transaction online.

DATES: To ensure consideration of comments, comments must be in writing and received by GSA no later than August 11, 2003.

ADDRESSES: Comments on this notice should be addressed to Ms. Von Harrison, General Services Administration; Office of Electronic Government and Technology (MEI), Washington, DC 20405. You are encouraged to submit these comments by facsimile to (202) 501–6455, or by electronic mail to *egov.taskforce@gsa.gov.*

FOR FURTHER INFORMATION CONTACT: Ms. Von Harrison, General Services Administration, Office of Electronic Government and Technology (MEI), Washington, DC 20405; or by phone at (202) 273–0721.

SUPPLEMENTARY INFORMATION: As required by the Government Paperwork Elimination Act of 1998 (Public Law 105–277), most transactions currently accomplished by filing a Government paper form will be converted to an electronic format. These transactions will require some type of identity verification or authentication before taking place. It is also important that these electronic transactions incorporate the appropriate level of security. This attached GSA policy guidance provides agencies with a policy for the use of electronic authentication (or e-authentication) in electronic transactions. As the Federal Government works to expand the use of information technology and e-government, trust in electronic transactions is especially critical.

This memorandum establishes a four level approach for authentication to ensure trustworthy electronic transactions and to fulfill Federal privacy and information security requirements. These four levels reflect an increasing degree of confidence in the identity presented and represent a range of authentication technologies. This guidance will promote for the public—

- Use of a standard set of criteria for assessing e-government transactions authentication requirements;
- Consistent terminology when discussing authentication and levels of assurance;
- Secure, easy-to-use, and consistent method for managing identity in electronic transactions with the Government;
- Burden reduction in Government services and Government filings;
- Reuse of credentials for access to multiple Government services;
- Clearly understood criteria for access to particular Government services; and
- Protection against fraud in online transactions with the Government.

Having a consistent e-authentication process and policy guidance will enable Federal Agencies to—

- Reduce authentication system development and acquisition costs, and reallocate labor resources used to develop such systems;
- Reduce the burden on the public in complying with repeated, duplicate or inconsistent processes of identity proofing;
- Make consistent authentication decisions;
- Promote public trust in the use of online service delivery;
- Use existing and future e-authentication processes, within their organizations or those that are available Governmentwide; and
- Reduce the number and type of electronic credentials that Federal employees, citizens, and businesses need to conduct business electronically with the Government.

This guidance updates the Procedures and Guidance for Implementing the Government Paperwork Elimination Act (GPEA) issued by the Office of Management and Budget (OMB), which requires agencies to provide the option for electronic filing and electronic signature capabilities for Government activities and services unless it is not practicable to do so by October 2003. The GPEA implementation guidance (found at: *http://www.whitehouse.gov/omb/memoranda/m00–10.html,* April 25, 2000), provided agencies with guidance on the risk factors agencies should consider in planning and implementing electronic transactions. This e-authentication policy updates the GPEA guidance to take in account current e-authentication practices, including the impacts of the E-Authentication E-Government Initiative and recent National Institute of Standards and Technology (NIST) standards. NIST will be issuing companion technical guidance on this issue.

This guidance reflects substantial work of the E-Authentication Initiative and the Federal CIO Council in FY 2003. Accordingly, CIOs are responsible for assuring all agencies or cross agency teams that implemented electronic authentication solutions or are planning to use shared authentication services are applying this policy.

All existing transactions/systems which require authentication of their users must complete an e-authentication risk assessment and be categorized into one of the described assurance levels by September 15, 2005. Agencies should complete the e-authentication risk assessment process in the following order:

- The E-Government Initiatives (who have already started the process described in this guidance) must be completed by October 1, 2003.
- Systems classified as ''major'' should be completed by September 15, 2004.
- New authentication solutions should begin to be categorized within 90 days of the completion of the final E-Authentication Technical Guidance.

The results of the authentication risk assessment must be made publicly available through the agency Web site, the **Federal Register**, or other means (*e.g.*, upon request). As part of the E-Authentication Initiative, E-Authentication will post the results of the assessments at a central location to allow for public access. In addition, the Business Compliance One Stop Initiative will be working with agencies' applications that concern small businesses. Agencies will be asked to report on their process as part of the requirements of Section 203 of the E-Government Act in the annual E-Government Act report due annually on September 15th beginning in 2004. Your cooperation and comments are appreciated.

Dated: July 8, 2003.

G. Martin Wagner,

Associate Administrator for Governmentwide Policy.

Draft E—Authentication Policy for Federal Agencies

1. Introduction

1.1. Summary

• This guidance should be applied to all Federal electronic transactions requiring authentication, except those that are national security systems as defined in 44 U.S.C. 3542(b)(2).

• This guidance does *not* stipulate which technology solutions should be implemented for each assurance level. The Department of Commerce's National Institute for Standards and Technology (NIST) is developing complementary e-authentication technical guidance that will be used by agencies to determine appropriate technology solutions, based on the process described in this guidance.

• Agencies are required to review existing and categorize new electronic transactions to ensure that these transactions comply with this guidance.

• As detailed in Section 9c of OMB's GPEA guidance, agencies should continue to minimize the likelihood of denial or repudiation of the information individuals transmit electronically. As an element of assessing the risks that are relevant to the required assurance level, agencies must consider how they plan to minimize the likelihood of repudiation by ensuring the user's approval of the information transmitted in electronic transactions. General guidance on minimizing the likelihood of repudiation is included in Section 8c of the OMB Procedures and Guidance on Implementing GPEA.

• This guidance does not directly apply to authorization. Authentication focuses on establishing a person's identity, based on the reliability of the credential he or she offers; while authorization focuses on what actions that identity, at that level of assurance, is permitted to do. Decisions concerning authorization are and should remain the purview of the electronic business process owner.

• Authentication is an inherent part of an electronic signature; however this guidance does not cover ''intent to sign,'' or when an agency uses authentication credentials as an electronic signature. For more information on electronic signatures, please consult OMB's guidance on implementing GPEA and the Electronic Signatures in Global and National Commerce Act (found at: *http://www.whitehouse.gov/omb/memoranda/m00–15.html,* September 25, 2000).

• Agencies should implement an e-authentication process using the following steps, described in Section 2.2: (1) Conduct a risk assessment as explained in Part II of the GPEA guidance and Section 2 of this guidance, (2) match identified risks with assurance levels, and (3) determine implementation technology based on the e-authentication technical guidance.

• Each step of the authentication process—from identity proofing, to issuance of a credential, to technical and administrative management and use of the credential by an application, and ultimately to record keeping and auditing—influences whether the process conforms to the desired assurance level. There are many layers of risk related to authentication. This guidance document is intended to assist agencies in identifying and analyzing risks associated specifically with the improper authentication of users of electronic transactions. These risks are highly dependent on the type of application and transactions offered.

• This document does not address risks that are associated with the improper management of authentication controls or processes, or risks to the underlying authentication technical architecture or infrastructure. 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.

• This guidance does not refer to the authentication of systems or between services (for example, security socket layer (SSL) authentication). Instead, it is focusing on the attribute or identity authentication of individuals who are authenticated for Government services online.

1.2. Overview

This document provides agencies with guidance on electronic identity and attribute authentication (or e-authentication). E-authentication is the process of establishing confidence in both identities and attributes after being electronically presented to an information system. Individual authentication is the process of establishing an understood level of confidence that an identifier refers to a specific individual. Attribute authentication is the process of establishing an understood level of confidence that an attribute applies to a specific individual. The process of e-authenticating an individual may involve establishing the individual's unique identity (identity authentication) or establishing that the individual is a member of a group (such as a military veteran or U.S. citizen) (attribute authentication). For a complete list of definitions, refer to the Report of the National Research Council ''Who Goes There? Authentication Through the Lens of Privacy'' (found at: *http://www.nap.edu/books/0309088968/html/,* March 31, 2003).

E-authentication is the first step in the related process of deciding what an individual ought to be allowed to do, called ''authorization.'' Authentication focuses on establishing a person's identity, based on the reliability of the credential he or she offers; while authorization focuses on what actions that identity is permitted to do.

Agencies providing the e-government services need to determine how certain they need to be in the identity of an individual and identify the risks inherent in a particular transaction. This guidance will provide the framework for the identified risks to be mapped to the desired assurance level that the authentication technology selected must satisfy.

As described in OMB Circular A–130, Management of Federal Information Resources, agencies must prepare and update a strategy that identifies and mitigates risks associated with each information system; Section 5 of the GPEA guidance detailed the risk factors agencies should consider in planning and implementing electronic transactions. This new e-authentication guidance expands on Section 5 by—

• Instructing agencies how to implement an e-authentication process by outlining a process for assessing risk, and determining the requisite level of identity assurance; and

• Describing four discrete (and increasing) levels of identity assurance.

2. Assurance Levels

2.1. Description of Assurance Levels

For the purposes of e-government transactions, this guidance describes four assurance levels for authentication. In this context, assurance is defined as how much confidence the relying party has that the electronic identity credential presented is done so by the person whose identity is asserted by the credential. These levels are each appropriate for different classes of electronic transactions. In general, informal or lower value transactions will require less stringent assurance levels. Higher value or legally significant transactions will require more stringent assurance levels.

2.2. How To Determine an Assurance Level

Step 1: Agencies should conduct a systematic risk assessment of the transaction. The risk assessment will determine the required assurance level and will measure the relative severity of the potential harm to the agency or user of the e-government application and other transaction participants in the event of an improperly validated or unauthorized authentication. Each of the 4 levels described in Section 2.4 contains a profile of consequential risks. The more severe the likely consequences, the more confidence required in the asserted electronic identity in order to engage in a transaction, and, therefore, the higher the assurance level required. The definition of each assurance level is directly correlated to the degree of confidence or certainty that the agency must have in the identity of the user. Assurance levels are the vital link between the risk assessments of applications and the selection of authentication solutions.

Agencies should consider a wide range of possible scenarios in seeking to determine what risks are associated with their business process. It is better to be over inclusive than under inclusive in conducting this analysis. Risk analysis is to some extent a creative process, in which agencies must consider harms that might result from, among other causes, technical failures, malignant third parties, public misunderstandings, and human error.

Step 2: Match identified risks with assurance levels. The results of the risk assessment should be summarized, and then

be directly compared to these profiles. The closest match to one of the level profiles will determine the assurance level. In determining the required assurance level, an agency should initially identify risks inherent in the transactional process without considering the particular technologies used to implement authentication for that transaction. For example if during a medical procedure, the misuse of a user's electronic identity/credentials might result in risk to the user's personal safety, then, following this guidance, the agency would assign a level 4 assurance to this transaction, even if potential financial loss or other consequences are minimal. In making this determination, business process owners should seek to use the minimum assurance level that meets their risk requirements.

Step 3: Determine implementation technology based on the e-authentication technical guidance. After the assurance level has been determined, the agency should refer to the e-authentication technical guidance for the process requirements corresponding to that level. After the technical solution is chosen, a final validation should be conducted to confirm that the required assurance level of the end-to-end user to agency process has been operationally achieved. Note that authorization determines whether or not the authenticated has rights to complete the transaction.

Note that some technology solutions may create or compound particular risks. Thus, after selecting a specific solution, the agency should validate that the performance of the authentication process itself actually meets the identity assurance requirements for the transaction as part of required security procedures (*e.g.*, certification and accreditation).

2.3. Assurance Levels: Descriptions and Examples

This section describes the four assurance levels. The levels represent ranges of confidence in an electronic identity presented to an agency by means of a credential. The levels are numbered from 1 to 4, with 1 being minimal assurance and 4 being the highest level of identity assurance.

For each level, there is a description and examples. The description and examples will assist the agency in identifying the appropriate level of assurance required to authorize a transaction. The key part of each description is a risk profile. This is a description of certain consequential risks that may ensue to participants in a transaction when there is an authentication error.

Level 1—Minimal Assurance

Description

At level 1, little or no assurance is placed in the asserted electronic identity of the transacting party. In particular, an authentication error of a user's identity at level 1 might result in at most—

- Minimal inconvenience to any party; and
- No financial loss to any party; and
- Minimal distress being caused to any party; and
- Minimal damage to any party's standing or reputation; and
- No risk of harm to agency programs or other public interests; and
- No risk of civil or criminal violations; and
- No release of personal, U.S. government sensitive, or commercially sensitive data to unauthorized parties; and
- No risk to any party's personal safety.

Examples

Examples of transactions that might merit level 1 authentication include—

- A user presents a self registered user ID or password to the United States Department of Education web page, which allows customization of a Web site to create a ''My.ED.gov'' page. There are some possible risks associated with this situation; for example, a third party who gained unauthorized access to such a user ID and password might be able to draw inferences about the user's business interests or plans or the user's personal situation based on the types of information in which the user has an interest. Unless the website is subject to a high degree of customization, however, these risks are probably very minimal.
- A user participates in an online discussion on the whitehouse.gov website. Assuming that the forum is not one that addresses sensitive or private information, there are no obvious risks associated with this situation.

Level 2—Low Assurance

Description

Level 2 is appropriate for transactions in which it is sufficient that, on the balance of probabilities, there is confidence in the asserted electronic identity of the transacting party. In particular, an authentication error of a user's identity at level 2 might result in—

- Minor inconvenience to any party; or
- Minor financial loss to any party; or
- Minor damage to any party's standing or reputation; or
- Minor distress being caused to any party; or
- Minor risk of harm to agency programs or other public interests; or
- A risk of civil or criminal violations of a nature that would not ordinarily be subject to agency enforcement efforts; or
- A minor release of personal, or commercially sensitive data to unauthorized parties; and
- No release of U.S. government sensitive data to unauthorized parties; and
- No risk to any party's personal safety.

Examples

Examples of transactions that might merit level 2 assurance include—

- A user engages in online learning on the Gov Online Learning Center at golearn.gov. There is a need for authentication such that the user is recognized by the training service and be connected to the appropriate place in the course or given relevant assignment grades, when training affects compensation or promotion. The only risk associated with this transaction is that a third party will gain access to grading information, causing harm to the privacy interests or reputation of the student. If the agency determines, in the context of the particular program, that any such harm will be minor, the transaction is level 2.
- A user accesses their Social Security retirement account information online.

Level 3—Substantial Assurance

Description

Level 3 is appropriate for transactions that are official in nature, and for which there is a need for high confidence in the asserted electronic identity of the transacting party. In particular, an authentication error of a user's identity at level 3 might result in—

- Significant inconvenience to any party; or
- Significant financial loss to any party; or
- Significant damage to any party's standing or reputation; or
- Significant distress being caused to any party; or
- Significant harm to agency programs or other public interests; or
- A risk of civil or criminal violations that may be subject to agency enforcement efforts; or
- A significant release of personal, U.S. government sensitive, or commercially sensitive data to unauthorized parties; and
- No risk to any party's personal safety.

Examples

Examples of transactions that might merit level 3 assurance include:

- A patent attorney company reports and updates data on-line with the Patent and Trademark Office that would be of great value as competitive intelligence.
- A major contractor or supplier maintains an account with a General Services Administration Contracting Officer for a large government procurement involving significant government expenditures.
- A First Responder accesses a disaster management reporting website to report an incident and to share incident operational information, and to coordinate incident response activities.

Level 4—High Assurance

Description

Level 4 is appropriate for transactions that are official in nature for which there is a need for very high confidence in the asserted electronic identity of the transacting party. In particular, an authentication error of a user's identity at level 4 might result in—

- Considerable inconvenience to any party; or
- Considerable financial loss to any party; or
- Considerable damage to any party's standing or reputation; or
- Considerable distress being caused to any party; or
- Considerable harm to agency programs or other public interests; or
- A risk of civil or criminal violations that are of special importance to the agency enforcement program; or
- A damaging release of extensive personal, U.S. government sensitive, or commercially sensitive data to third parties; or
- A risk to any party's personal safety.

Examples

Examples of transactions that may require level 4 assurance include—

• A State or local law enforcement official accesses a law enforcement database containing information about the criminal records of individuals. Unauthorized access would violate the legal privacy rights of individuals or compromise investigations.

• A VA pharmacist dispenses a controlled drug. He/She would need full assurance that a qualified doctor had signed the prescription. In this case, the pharmacist's actions on the transaction carries criminal liability that the prescription was the correct drug(s), in the correct quantity, and that the prescription was validated before filling the prescription.

2.4. Additional Considerations

Each step of the authentication process—from identity proofing, to issuance of a credential, to management and use of the credential in a well-managed secure application, and ultimately to record keeping and auditing—influences whether the process conforms to the desired assurance level. The level of assurance achieved by each step of the process needs to be considered. The step that provides the lowest level of assurance may often determine the assurance level for the entire authentication process. Ideally each step in the authentication process should be consistent in its strength and robustness. A strong identity proofing process, combined with a strong credential and a robust management practice (including a strong archive and audit process) will contribute to the highest level assurance of identity. However, the best authentication process needs to be supported by well-engineered and tested user and agency software applications.

In making the risk assessment, the business process owner must consider all the direct and indirect consequences as presented in the definitions of the levels. Since each assurance level uses the terms ''minimal'', ''minor'', ''significant'', or ''considerable'', the business process owner will need to consider the terms in the context of the parties likely to be affected and their typical views. While it is realized that these terms are subjective, it is expected that these will be solidified through implementation and practice. For example, risk assessments have already been conducted on the E-Government Initiatives to determine their appropriate assurance levels.

As stated in OMB's GPEA guidance, properly implemented technologies can offer degrees of confidence in authenticating identity that are greater than a handwritten signature can offer. However, electronic transactions may in some circumstances affect the risk of criminal and civil violations, increase the harms associated with such violations, and complicate redressing such violations. Legal and law enforcement issues are discussed in the Department of Justice's Guide for Federal Agencies on Implementing Electronic Processes (found at *http://www.cybercrime.gov/ecommerce.html#GFA, November 2000*). Agencies should consider these issues in assigning transactions to particular assurance levels.

Violations of the law can present significant policy issues for an agency. The risk assessment process should consider the potential effects of illegal activities or other process failures in light of the agency's enforcement priorities, the agency's programmatic interests, and such broader public interests as national security, the environment, and the proper functioning of markets. Some of these harms are specifically described in each level (such as financial loss or release of personal information); others will depend on a particular agency's programmatic interests.

The risk analysis reflects this issue by referring to risks of criminal or civil violations and harm to agency programs or the public interest. In assessing this risk and designing a process, agencies should take into account not just the effects of a single violation or other act, but the possibility of a pattern of actions that might affect agency programs. For instance, if sensitive information could be obtained from an agency website, the agency should consider the effects of a possible pattern of such activity, not just a single action, in assessing risk levels. (Note that unauthorized access to an agency website is itself a criminal offense, see, *e.g.,* 18 U.S.C. 1029, 1030. Agencies should consider the effects and risks associated with such unauthorized access, rather than focusing on the unauthorized access itself, in assessing such risks.)

3. Determining Assurance for Credential Service Providers

Credential Service Providers (CSPs) are organizations, both governmental and non-governmental, that issue and in some cases may maintain electronic credentials. CSPs can handle several of the steps in the e-authentication process. Because the CSP's issuance and maintenance policy influences the trustworthiness of an e-authentication process, CSPs will also need to be assessed to determine the e-authentication level to which their credentials pertain. For example, if a CSP follows all process/technology requirements for authentication level 3, a user may use a credential provided by the CSP to authenticate himself for a transaction requiring authentication levels 1, 2, or 3. Additional information on CSPs will be included in both the E-Authentication technical guidance and in separate guidance issued by the E-Authentication E-Government Initiative.

4. Implementing an Authentication Process

4.1. Overview of the E-Authentication Process

When determining e-authentication needs, agencies must consider the entire e-authentication process. An agency cannot simply determine the level of credential that will be required to validate a user's identity without also determining how that credential will be processed by the agency business applications. They must determine the requirements for each step in the e-authentication/authorization process. This process includes the following steps:

- Initial enrollment.
- Repeat visits.
- Verification of identity.
- Transaction management.
- Long term records management.
- Periodic tests of the system.
- Suspension, revocation, reissue.
- Audit.

Each of these steps will be explained in more detail in the e-authentication technical guidance. Responsibility for these steps lies with the individual business process owners or designated agency or cross agency authority.

4.2. Use of Anonymous Credentials

Anonymous credentials may be appropriate when it is not necessary that authentication be associated with a known personal identity (as opposed to identity authentication). To protect privacy, it is important to balance the need to know who is communicating with Government with a citizen's right to privacy. This includes ensuring that information is used only in the manner in which individuals have been assured it will be used. In some cases, it may be desirable to preserve the anonymity of individuals and it may be sufficient for the purposes of an application to authenticate that—

• The user is a member of a group; and/or

• The user is the same individual who supplied or created information in the first place; and/or

• A particular user is entitled to use a particular pseudonym.

These anonymous credentials will have limited application. In some cases, individuals would have an anonymous as well as a non-anonymous credential. Anonymous credentials can be used up until level 3.

4.3. Information Sharing and the Privacy Act

When developing authentication processes, agencies must consider the requirements for managing security in the collection and storage of information associated with the process of validating a user's identity. As required by the E-Government Act of 2002 (Public Law 107–347), section 208, 44 U.S.C. § 3604, agencies are required to conduct privacy impact assessments for electronic information systems and collections, which includes when authentication technology is newly applied to an electronic information system.

The following information is captured in most e-authentication processes:

• 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.

Some of this information includes personal information as defined by the Privacy Act and, systems that use the information are considered systems of records that must meet all requirements of the Privacy Act and the E-Government Act.

Data collected and stored during the authentication process should only be accessible routinely to systems administrators and to auditors. As required by the Privacy Act, access to the system of

records must be provided to registered users to allow them to see and/or change personal information about them maintained in the system of records. Information from the system of records should not be shared routinely outside of legitimate needs as permitted or required by law for the administration and control of the authentication process.

In order to authenticate a user, it may be necessary for an agency providing an E-Gov service to obtain additional information about that user through the CSP that issued the user his/her credential. In such a case, the CSP must ask the user for permission and be granted that permission by the user to provide the specified information to the e-gov service provider. Disclosure of the additional information by the CSP to the e-gov application or service may also be established prior to the time of the transaction, if it is outlined in the terms of the relationship between the user and the CSP.

4.4. Cost Considerations

In most cases, higher levels of assurance require more costly credentials; however minimizing the number of credentials can create cost savings. Section 3 of the GPEA guidance provides additional information on assessing risks, costs, and benefits. In-person proofing is most likely more expensive. The e-authentication technical guidance will provide alternatives for addressing some of the authentication levels that may help agencies to better manage the costs of authentication.

4.5. Relationship to Other Guidance

4.5.1. Federal Bridge Certification Authority

Federal Bridge levels will be mapped to the assurance levels described in this document. Since these assurance levels take into account a wide range of authentication solutions, the levels described in this guidance differ from the levels established by the Federal Bridge Certification Authority (FBCA) Certificate Policy. For example, levels 1 and 2 in this e-authentication policy are primarily reserved for non-cryptographic authentication solutions not covered by the FBCA. However, it is likely that some public key infrastructure (PKI) solutions and the FBCA Rudimentary Certificate Policy will map to level 1 or level 2. The FBCA Basic Certificate Policies and the FBCA Medium Certificate Policies will fall in level 3, while FBCA High Certificate Policy will fall into level 4.

4.5.2. Federal Information Processing Standards Publication 199

While this E-Authentication Guidance addresses the consequential risk in making an authentication error, NIST is in the process of developing much broader risk levels for Federal information and Information Systems. NIST is in the process of developing a Federal Information Processing Standards Publication (FIPS) 199, ''Standards for Security Categorization of Federal Information and Information Systems'' promulgated under the E-Government Act of 2002 (Public Law 107–347). The standards establish three levels of risk (low, moderate, and high) for each of the stated security objectives (confidentiality, integrity, and availability) relevant to securing Federal information and information systems.

It is expected that these levels established in FIPS 199 will map to the levels in the e-authentication guidance. When an authentication error might cause a loss of confidentiality, integrity or availability, then—

- If the risk as defined in FIPS 199 is low, authentication assurance levels 1 through 4 are sufficient;
- If the risk as defined in FIPS 199 is moderate, authentication assurance level 3 or 4 should be used; and
- If the risk as defined in FIPS 199 is high, authentication assurance level 4 should be used.

5. Effective Dates of This Guidance

The Effective Dates for this guidance is 30 days after issuance as final policy. Additional information can be found in the supplemental information above.

[FR Doc. 03–17634 Filed 7–10–03; 8:45 am]

BILLING CODE 6820–WY–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Disease Control and Prevention

Disease, Disability, and Injury Prevention and Control Special Emphasis Panel: Research To Improve Smoke Alarm Maintenance and Function, Program Announcement 03100

In accordance with section 10(a)(2) of the Federal Advisory Committee Act (Pub. L. 92–463), the Centers for Disease Control and Prevention (CDC) announces the following meeting:

Name: Disease, Disability, and Injury Prevention and Control Special Emphasis Panel (SEP): Research to Improve Smoke Alarm Maintenance and Function, Program Announcement 03100.

Times And Dates: 6:30 p.m.–7 p.m., July 27, 2003 (Open). 7 p.m.–8 p.m., July 27, 2003 (Closed). 8:30 a.m.–5 p.m., July 28, 2003 (Closed).

Place: The Swissotel Atlanta Buckhead, 3391 Peachtree Road, NE., Atlanta, GA 30326, Telephone 404.365.0065.

Status: Portions of the meeting will be closed to the public in accordance with provisions set forth in section 552b(c)(4) and (6), Title 5 U.S.C., and the Determination of the Director, Management Analysis and Services Office, CDC, pursuant to Public Law 92–463.

Matters To Be Discussed: The meeting will include the review, discussion, and evaluation of applications received in response to Program Announcement 03100.

FOR FURTHER INFORMATION CONTACT: Jean Langlois, Sc.D., Epidemiologist, Division of Injury and Disability Outcomes and Programs, National Center for Injury Prevention and Control, CDC, 4770 Buford Highway, NE, Atlanta, GA 30341, Telephone 770.488.1478.

The Director, Management Analysis and Services Office, has been delegated the authority to sign **Federal Register** notices pertaining to announcements of meetings and other committee management activities, for both CDC and the Agency for Toxic Substances and Disease Registry.

Dated: July 7, 2003.

Diane C. Allen,

Acting Director, Management Analysis and Services Office, Centers for Disease Control and Prevention.

[FR Doc. 03–17560 Filed 7–10–03; 8:45 am]

BILLING CODE 4163–18–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Disease Control and Prevention

Disease, Disability, and Injury Prevention and Control Special Emphasis Panel: Community-Based Interventions To Reduce Motor Vehicle-Related Injuries, Program Announcement 03077

In accordance with section 10(a)(2) of the Federal Advisory Committee Act (Pub. L. 92–463), the Centers for Disease Control and Prevention (CDC) announces the following meeting:

Name: Disease, Disability, and Injury Prevention and Control Special Emphasis Panel (SEP): Community-Based Interventions to Reduce Motor Vehicle-Related Injuries, Program Announcement 03077.

Times and Dates: 6:30 p.m.–7 p.m., July 27, 2003 (Open). 7 p.m.–8: p.m., July 27, 2003 (Closed). 8:30 a.m.–5 p.m., July 28, 2003 (Closed).

Place: The Swissotel Atlanta Buckhead, 3391 Peachtree Road, NE., Atlanta, GA 30326, Telephone 404.365.0065.

Status: Portions of the meeting will be closed to the public in accordance with provisions set forth in section 552b(c)(4) and (6), Title 5 U.S.C., and the Determination of the Director, Management Analysis and Services Office, CDC, pursuant to Public Law 92–463.

Matters to be Discussed: The meeting will include the review, discussion, and evaluation of applications received in response to Program Announcement 03077.