

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.