

Government Paperwork Elimination Act

This Act, and the implementing guidelines from the Office of Management and Budget (OMB), raise a series of complex issues and any final decisions regarding the appropriateness of implementation processes for the Act should be reviewed by authoritative legal counsel. This summary is not an exhaustive or authoritative one and is instead intended only to capture broad issues.

Near-term requirement

To ensure a smooth and cost-effective transition to an electronic government that provides improved service to the public, each agency must develop a plan (including a schedule) by October, 2000 that provides for continued implementation, by the end of Fiscal Year 2003, of optional electronic maintenance, submission, or transaction of information when practicable as a substitute for paper, including through the use of electronic signatures when practicable. The plan must address, among other things (and where applicable), the optional use by employers of electronic means to store and file with Federal agencies information about their employees. The plan should prioritize agency implementation of systems or modules of systems based on achievability and net benefit. The plan must be an addition to the agency's strategic IT planning activities supporting program responsibilities, as required by OMB Circular A-11. A copy of the plan should be provided to OMB.

Background

The Government Paperwork Elimination Act (GPEA) of October 21, 1998 establishes the requirement for government agencies to provide for electronic submission, maintenance, or disclosure of information as a substitute for paper and for the use and acceptance of electronic signatures. The term "electronic signature" was defined to mean a method of signing an electronic message that identifies and authenticates a particular person as the source of the electronic message and indicates such person's approval of the information contained in the electronic message.

OMB was directed to periodically report to Congress the results of an ongoing study of the use of electronic signatures under this Act that addresses:

1. paperwork reduction and electronic commerce;
2. individual privacy; and
3. the security and authenticity of transactions.

Primary Policy Documents

After a period of public comment, the final OMB implementation instructions for GPEA were issued on May 2, 2000. Rather than providing specific guidance, OMB suggests that certain existing policies provide a broad, common framework for ensuring the implementation of electronic systems in a secure manner. In various sections of the guidance document, OMB refers to, and recommends compliance with, the 35 documents set out in Appendix A. To fully comply with OMB's guidance, each Department or

agency must review and maintain familiarity with the changing landscape of these guidance documents.

Required Actions

The GPEA requires Federal agencies to provide individuals or entities the option to submit information or transact with the agency electronically and to maintain records electronically when practicable. It also encourages Federal government use of a range of electronic signature alternatives. This process must be in place by October 2003.

The GPEA charged OMB with developing procedures for Executive agencies to follow in using and accepting electronic documents and signatures. This includes records required to be maintained under Federal programs and information that employers are required to store and file with Federal agencies about their employees. These procedures reflect and are to be executed with due consideration of the following policies:

1. maintaining compatibility with standards and technology for electronic signatures generally used in commerce and industry and by State governments;
2. not inappropriately favoring one industry or technology;
3. ensuring that electronic signatures are as reliable as appropriate for the purpose in question;
4. maximizing the benefits and minimizing the risks and other costs;
5. protecting the privacy of transaction partners and third parties that have information contained in the transaction;
6. ensuring that agencies comply with their record keeping responsibilities under the FRA for these electronic records. Electronic record keeping systems reliably preserve the information submitted, as required by the Federal Records Act and implementing regulations; and
7. providing, wherever appropriate, for the electronic acknowledgment of electronic filings that are successfully submitted.

Implementation Expectations

Agencies are instructed to conduct an assessment of whether to use and accept documents in electronic form and to engage in electronic transactions. The assessment should weigh costs and benefits and involve an appropriate risk analysis, recognizing that low-risk information processes may need only minimal consideration, while high-risk processes may need extensive analysis. Agencies should develop and implement electronic transaction plans on the basis of this assessment.

The assessment should evaluate electronic signature alternatives on the basis of the guidance documents cited by OMB. The assessment should not be an isolated activity and should develop strategies to mitigate risks, maximize benefits, and develop verifiable performance measures tied to agency strategic plans and Clinger-Cohen Act performance measures. Assessments should include a cost evaluation and should be designed to

generate a verifiable return on investment to support implementation decisions and must be completed for each information system.

Risk Assessment Requirements

Mitigation of risk is a common theme throughout OMB guidance, but based on a demonstrable need that balances the relative costs, risks, and benefits given the level of sensitivity of the transaction and the process(es) the system supports. The required risk analyses are envisioned to use a combination of quantitative and qualitative methods to judge the practicability of any electronic transaction method and are expected to be comprehensive if the transaction or the data are particularly sensitive.

The recommended quantitative approach to risk analysis should attempt to estimate the monetary cost of risk compared to the cost of risk reduction techniques base on:

1. the likelihood that a damaging event will occur,
2. the costs of potential losses, and
3. the costs of mitigating actions that could be taken.

Since reliable data on likelihood and costs may not be available, a qualitative approach may be taken by defining risk in more subjective and general terms, such as High, Medium, and Low. Such qualitative analyses depend more on the expertise, experience and good judgment of the person conducting the assessment.

The risk factors to be considered in planning and implementing electronic signatures or electronic transactions are specifically identified by OMB. They include the following types of transactions, each of which is perceived by OMB as potentially having differing security risks:

1. What is the relationship between the parties?
 - a) Intra-agency transactions?
 - b) Inter-agency transactions?
 - c) Transactions with a state or local government?
 - d) Transactions private organizations?
 - e) Transactions with a member of the general public?
 - f) Transactions with a foreign government?
2. What is the value of the transaction?
 - a) A transaction that involves the transfer of funds?
 - b) A transaction where the parties commit to actions or contracts that create a financial or legal liability?
 - c) A transaction involving information protected under the Privacy Act or national security information?
 - d) A transaction where the party is fulfilling a legal responsibility which, if not performed, creates a legal liability (criminal or civil)?
 - e) Other transactions.

3. What is the risk/probability of intrusion?
 - a) Is it a regular or periodic transaction?
 - b) What is the value of the information to outside parties?
 - c) Is the perceived image or mission of the agency one that may make it more likely to be attacked?
4. What is the need for accessible, persuasive information regarding the transaction at a later point?
 - a) Will the information be used for a short time and discarded?
 - b) May the information later be subject to audit or compliance review?
 - c) Will the information be used for research, program evaluation, or other statistical analyses?
 - d) Might the information later be subject to dispute by a party or alleged party to the transaction?
 - e) Might a non-party to the transaction have reason to dispute the information?
 - f) Might the information be needed as proof in court?
 - g) Will the information be archived as permanently valuable records?

Privacy and Disclosure Issues

The GPEA limits the use of information collected in electronic signature services to communications with a Federal agency. It directs agencies and their staff and contractors not to use such information for any purpose other than for facilitating the communication. Accordingly, agencies should follow several privacy principles:

1. Electronic signatures should only be required where needed.
2. When electronic signatures are required for a transaction, agencies should not collect more information from the user than is required for the application of the electronic signature. When appropriate, agencies are encouraged to use methods of electronic signing that do not require individuals to disclose their identity.
3. Users should be able to decide how, when, and what type of electronic authentication to use of those made available by the agency. If none are acceptable the user should be able to opt out to a paper process.
4. Agencies should ensure, and users should be informed, that information collected for the purpose of issuing or using electronic means of authentication will be managed and protected in accordance with applicable requirements.

Possible Electronic Transaction Technologies

OMB's guidance addresses cryptographic and non-cryptographic methods of authenticating identity. To be effective, these electronic transaction authentication methods require agencies to develop a series of policy documents that provide the important underlying framework for electronic transactions and which facilitate the evaluation of risk.

In considering the underlying policies for mitigating risk to authentication of electronic transactions, policies and procedures that ensure the integrity of security tools helps counter attempts to defraud. For example, transactions which appear to be at high risk for fraud, e.g., one-time high-value transactions with persons not previously known to an agency, may require extra safeguards or may not be appropriate for electronic transactions.

The spectrum of electronic signature technologies OMB perceives as being currently available are as follows.

1. A Personal Identification Number (PIN) or password. The system checks that password or PIN against data in a database to ensure its correctness and thereby "authenticates" the user.
2. Secure Sockets Layer (SSL) with PIN or password. SSL uses a combination of public key technology and symmetric cryptography to automatically encrypt information as it is sent over the Internet by the user and decrypt it before it is read by the intended recipient.
3. Smart Card. A smart card can be used to facilitate various authentication technologies all embedded on the same card. By having different authentication choices the user can pick the authentication technique that meets but does not exceed the information requirement for the transaction. One approach is that information from the card's chip is provided to the computer only when the user also enters a PIN, password, or biometric identifier recognized by the card. This method offers far greater security than the typical use of a PIN or password.
4. Digitized Signature (not to be confused with a Digital Signature). A digitized signature is a graphical image of a handwritten signature. Some applications require an individual to create his or her hand-written signature using a special computer input device, such as a digital pen and pad. The digitized representation of the entered signature may then be compared to a previously-stored copy of a digitized image of the handwritten signature. If special software judges both images comparable, the signature is considered valid.
5. Biometrics. Individuals have unique physical characteristics that can be converted into digital form and then interpreted by a computer. In this technology, the physical characteristic is measured (by a microphone, optical reader, or some other device), converted into digital form, and then compared with a copy of that characteristic stored in the computer and authenticated beforehand as belonging to a particular person.
6. Shared Symmetric Key Cryptography. In shared symmetric key approaches, the user signs a document and verifies the signature using a single secret key. Since the symmetric key is shared between the sender and possibly many recipients, it is not private to the sender and hence has lesser value as an authentication mechanism.
7. Public/Private Key (Asymmetric) Cryptography - Digital Signatures. To produce a digital signature, a user has his or her computer generate two mathematically

linked keys -- a private signing key that is kept private, and a public validation key that is available to the public. The public key is made part of a "digital certificate," which is a specialized electronic file digitally signed by the issuer of the certificate, binding the identity of the individual to his or her private key in an unalterable fashion

While digital signatures are generally the most certain method for assuring identity electronically, the policy documents must identify how well the signer's identity is bound to his or her public key in a digital certificate. The strength of this binding depends on the assumption that only the owner has sole possession of the unique private key used to make signatures that are validated with the public key. The strength of this binding also reflects whether the private key is placed on a highly secure hardware token, such as a smart card.

A Public Key Infrastructure (PKI) is one mechanism to support the binding of public keys with the user's identity. A PKI can provide the entire policy and technical framework for the systematic and diligent issuance, management and revocation of digital certificates.

Evaluation of Authentication Mechanisms

OMB provides the following summary of the process and principles that agencies should employ to evaluate authentication mechanisms:

1. Examine the current business process that is being considered for conversion to employ electronic documents, forms or transactions, identifying customer needs and demands as well as the existing risks associated with fraud, error or misuse.
2. Identify the benefits that may accrue from the use of electronic transactions or documents.
3. Consider what risks may arise from the use of electronic transactions or documents. This evaluation should take into account the relationships of the parties, the value of the transactions or documents, and the later need for the documents.
4. Consult with counsel about any agency specific legal implications about the use of electronic transactions or documents in the particular application.
5. Evaluate how each electronic signature alternative may minimize risk compared to the costs incurred in adopting an alternative.
6. Determine whether any electronic signature alternative, in conjunction with appropriate process controls, represents a practicable trade-off between benefits on the one hand and cost and risk on the other. If so, determine, to the extent possible at the time, which signature alternative is the best one. Document this determination to allow later reevaluation.
7. Develop plans for retaining and disposing of information, ensuring that it can be made continuously available to those who will need it, for managerial control of

- sensitive data and accommodating changes in staffing, and for ensuring adherence to these plans.
8. Develop management strategies to provide appropriate security for physical access to electronic records.
 9. Determine if regulations or policies are adequate to support electronic transactions and record keeping, or if "terms and conditions" agreements are needed for the particular application. If new regulations or policies are necessary, disseminate them as appropriate.
 10. Seek continuing input of technology experts for updates on the changing state of technology and the continuing advice of legal counsel for updates on the changing state of the law in these areas.
 11. Perform periodic review and re-evaluation, as appropriate.

Appendix A

After a period of public comment, the final OMB implementation instructions for GPEA were issued on May 2, 2000. Rather than providing specific guidance, OMB suggests that certain existing policies provide a broad, common framework for ensuring the implementation of electronic systems in a secure manner. In various sections of the guidance document, OMB refers to, and recommends compliance with, the following existing policy documents:

1. OMB Circular A-130 Appendix III as revised February 1996 entitled, “Security of Federal Information Resources.”
2. Presidential Decision Directive 63 of May 22, 1998.
3. *Access With Trust*, published by the Federal Public Key Infrastructure Steering Committee and OMB in September, 1998.
4. A Presidential Memorandum entitled, “Electronic Government” of December 1999.
5. The Computer Security Act of 1987 (40 USC § 759).
6. OMB Memorandum 99-20 entitled, “Security of Federal Automated Information Resources” of June 1999.
7. “Good Security Practices for Electronic Commerce, Including Electronic Data Interchange” published by the Department of Commerce, National Institute of Standards and Technology (NIST) as special publication 800-9 in December 1993.
8. NIST publication 800-12 entitled, “An Introduction to Computer Security: The NIST Handbook” of December 1995.
9. NIST publication 800-14 entitled, “Generally Accepted Principles and Practices for Security Information Technology Systems” of September 1996.
10. NIST publication 800-18 entitled, “Guide for Developing Security Plans for Information Technology Systems” of December 1998.
11. The General Accounting Office (GAO) publication GAO/AIMD-00-33 entitled, “Information Security Risk Assessment: Practices of Leading Organizations” of November 1999.
12. “ROI and the Value Puzzle” published by the Capital Planning and IT Investment Committee of the Federal CIO Council in April 1999.
13. OMB Memorandum 00-07 entitled, “Incorporating and Funding Security in Information Systems Investments” issued February 28, 2000.
14. The Privacy Act, 5 USC 552.
15. The Federal Records Act of 1950 and implementing regulations.
16. The Government Performance Results Act of 1993.
17. The Clinger-Cohen Act of 1996.

18. The Federal Managers' Financial Integrity Act
19. The Chief Financial Officers Act.
20. "Federal Information Processing Standards" promulgated by the Secretary of Commerce.
21. OMB Circular A-119 entitled, "Federal Participation in the Development and Use of Voluntary Consensus Standards and Conformity Assessment Activities" of February 1998.
22. OMB Circular A-11 Part 3 entitled, "Planning, Budgeting, and Acquisition of Capital Assets."
23. The Paperwork Reduction Act of 1995.
24. The Uniform Electronic Transactions Act adopted by the National Conference of Commissioners of Uniform State Laws.
25. The Federal Rules of Evidence, especially Chain of Custody.
26. Security and Exchange Commission electronic regulatory filings regulations 17 CFR Part 232.
27. Environmental Protection Agency policy on electronic reporting 55 Federal Regulations 31030 of 1990.
28. Food and Drug Administration electronic signatures and records 21 CFR Part 11.
29. Internal Revenue Service signature alternatives for tax filings Treasury Regulation 301.6061-1
30. Federal Acquisition Regulation electronic contracts 48 CFR Parts 2 and 4.
31. General Services Acquisition Regulation electronic orders 48 CFR Part 552.216-73.
32. Federal Property Management Regulations electronic bills of lading 41 CFR Part 101-41.
33. Administrative Committee of the Federal Register electronic signatures on documents submitted for publication in the Federal Register 1 CFR Part 18.7.
34. Commodity Futures Trading Commission electronic signatures for filings 17 CFR Part 1.4 and Part 1.3(tt).
35. "Performance Guidelines for the Legal Acceptance of Records Produced by Information Technology Systems" of the Association for Information and Image Management (ANSI/AIIM TR31).