OFFICE OF MANAGEMENT AND BUDGET

Management of Federal Information Resources

AGENCY: Office of Management and Budget, Executive Office of the President.

ACTION: Proposed Implementation of the Government Paperwork Elimination Act.

SUMMARY: The Office of Management and Budget (OMB) requests public and agency comment on proposed procedures and guidance to implement the Government Paperwork Elimination Act (GPEA). Under the GPEA, agencies must generally provide for the optional use and acceptance of electronic documents and signatures, and electronic record keeping where practicable, by October 2003.

DATES: Persons who wish to comment on the GPEA procedures and guidance should submit their comments no later than July 5, 1999. Each Department and Agency is asked to submit a single coordinated set of comments.

ADDRESSES: Electronic comments will be included as part of the official record. Please send comments electronically to: gpea@omb.eop.gov. Alternatively, hardcopy comments may be addressed to: Information Policy and Technology Branch, Office of Information and Regulatory Affairs, Office of Management and Budget, Room 10236 New Executive Office Building, Washington, D.C. 20503.

ELECTRONIC AVAILABILITY: This document is available on the Internet in the OMB library of the ''Welcome to the White House'' home page, http://www.whitehouse.gov/WH/EOP/OMB/, the CIO Council's home page, http://cio.gov, and at the Government Information Technology Services Board's security home page at http://gits-sec.treas.gov.

FOR FURTHER INFORMATION CONTACT: Peter Weiss, Information Policy and Technology Branch, (202) 395–3630. Press inquiries should be addressed to the OMB Communications Office, (202) 395–7254.

SUPPLEMENTARY INFORMATION: Public confidence in the security of the government's electronic information and information technology is essential in creating government services that are more accessible, efficient, and easy to use. Electronic commerce, electronic mail, and electronic benefits transfer sensitive information within government, between the government and private industry or individuals, and among governments. These electronic systems must protect the information's confidentiality, assure that the information is not altered in an unauthorized way, and be available when needed. A corresponding policy and management structure must support these protections.

In a major step in this direction, the Congress recently enacted legislation, supported by the Administration, intended to increase the ability of citizens to interact with the Federal government electronically. The Government Paperwork Elimination Act, Title XVII of Pub. L. 105–277, provides for Federal agencies, by October 21, 2003, to give persons who are required to maintain, submit, or disclose information the option of doing so electronically when practicable as a substitute for paper, and to use electronic authentication (electronic signature) methods to verify the identity of the sender and the integrity of electronic content. The Act specifically provides that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form.

OMB's proposed implementation of the Act is in two parts. The first part sets forth the policies and procedures for implementing the Act, and requesting certain specific agencies to provide assistance in particular areas. The second part is intended to provide Federal managers with practical implementation guidance.

OMB requests comments on the proposed procedures and guidance.

Donald Arbuckle,

Deputy Administrator and Acting Administrator, Office of Information and Regulatory Affairs.

Proposed OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act

This provides Executive agencies with the guidance needed to implement the Government Paperwork Elimination Act (GPEA), Pub. L. 105–277, Title XVII, which took effect on October 21, 1998. The GPEA is an important tool to fulfill the Administration's vision of improved customer service and governmental efficiency through the use of information technology. This vision, articulated in Vice President Gore's 1997 report, Access America (http://gits.gov), involves widespread use of the Internet, with Federal agencies transacting business electronically, in the same way as commercial enterprises. Those who wished to do business in this way could avoid traveling to government offices, waiting in line, or mailing paper forms. Delivery of government services in this way would normally save the government time and money as well.

Access America recognized, however, that:

Public confidence in the security of the government's electronic information and information technology is essential to creating government services that are more accessible, efficient, and easy to use. Electronic commerce, electronic mail, and electronic benefits transfer sensitive information within government, between governments and private industry or individuals, and among governments. These electronic systems must protect the information's confidentiality, assure that the information is not altered in an unauthorized way, and be available when needed.

Part I. Policy and Procedures

Section 1. Policy

The GPEA charges the Office of Management and Budget, in consultation with the Commerce Department and other appropriate entities, with the development of procedures for Executive agencies to follow in using and accepting electronic documents and signatures. These procedures reflect and are to be executed with due consideration of the following policies:

a. Maintaining compatibility with standards and technology for electronic signatures generally used in commerce and industry and by State governments;

b. not inappropriately favoring one industry or technology;

c. ensuring that electronic signatures are as reliable as is appropriate for the purpose in question and that electronic record keeping systems reliably preserve the information submitted;

d. providing wherever appropriate for the electronic acknowledgment of electronic filings that are successfully submitted; and

e. providing, to the extent feasible and appropriate, for multiple methods of electronic signatures or identifiers for the submission of such forms where the agency anticipates receipt of 50,000 or more electronic submittals of a particular form.

Section 2. Procedures

a. The GPEA recognizes that adoption of electronic systems should be consistent with the need to ensure that investments in information technology are economically prudent to accomplish the agency's mission and give due regard to privacy and security.

Moreover, it is Administration policy that a decision to not allow the option of electronic filing and record keeping should be supported by a specific showing that, in the context of a particular application, there is no reasonably cost-effective combination of technologies and management controls that can minimize the risk of significant harm. Accordingly, agencies should develop and implement plans to use and accept documents in electronic form, and engage in electronic transactions.

b. An agency's determination of which technology is appropriate for a given transaction must include a risk assessment, and an evaluation of targeted customer or user needs. Performing a risk assessment to evaluate electronic signature alternatives should not be viewed as an isolated activity or an end in itself. These agency risk assessments should draw from and feed into the interrelated requirements of the Paperwork Reduction Act, the Computer Security Act, the Government Performance and Results Act, the Clinger-Cohen Act, the Federal Managers Financial Integrity Act, and the Chief Financial Officers Act.

c. The initial use of the risk assessment is to identify and mitigate risks in the context of available technologies and their relative total costs and effects on the program being analyzed. The assessment also should be used to develop baselines and verifiable performance measures that track the agency's mission, strategic plans, and tactical goals.

d. The analysis of costs and benefits should be designed so that it can be used, not only as a guide to selecting among the technologies under consideration, but also to generate a business case and verifiable return on investment to support decisions regarding overall programmatic direction, investment decisions, and budgetary priorities. The effects on the public and its needs and readiness to move to an electronic environment are important considerations.

Section 3. Agency Responsibilities

a. In order to ensure a smooth and cost-effective transition to a more electronic government providing improved service to the public, each agency shall:

1. Include in its strategic IT plans supporting program responsibilities (required under OMB Circular A–11) a summary of the agency's schedule to implement optional electronic maintenance, submission, or disclosure of information when practicable as a substitute for paper, including through the use of electronic signatures when practicable, by the end of Fiscal Year 2003 (note: agencies need not revise their reports on Federal purchasing and payment already required by OMB M–99–02, but should include the automation of purchasing and payment functions in their schedule);

2. consider whether an appropriate combination of information security practices, authentication technologies and management controls for each application will be practicable, and if so, which combination will minimize risk and maximize benefits in a cost effective manner;

3. promulgate or amend regulations or policies as necessary and appropriate to: (1) Implement optional electronic submission, maintenance, or disclosure of information, and the use of any necessary electronic signature alternatives; and (2) permit private employers who have record keeping responsibilities imposed by the Federal government to electronically store and file information pertaining to their employees electronically;

4. maintain appropriate information system confidentiality and security in accordance with the guidance contained OMB Circular A–130, Appendices I and III, and use, to the maximum extent practicable, technologies either prescribed in Federal Information Processing Standards promulgated by the Secretary of Commerce or supported by voluntary consensus standards as defined in OMB Circular A–119;

5. provide, to the extent feasible and appropriate, more than one electronic signature option for public reporting forms which are collected annually in electronic form from more than 50,000 respondents; and

6. report progress against the strategic plans developed in response to 1. above through the annual agency reports submitted to OMB under the Paperwork Reduction Act, including any determination that a particular application is inappropriate for conversion to electronic filing.

(b) Department of Commerce.

The Department of Commerce shall promulgate Federal Information Processing Standards as appropriate to further the specific goals of the GPEA. The Department should also develop best practices in the area of authentication technologies and implementations, including cryptographic digital signature technology, with assistance from the Government Information Technology Services Board, the Chief Information Officers Council and the President's Management Council.

(c) Department of the Treasury.

The Department of the Treasury shall prescribe policies and practices for the use of electronic authentication techniques in Federal payments and collections, and ensure that they fulfill the the goals of GPEA.

(d) Department of Justice.

The Department of Justice shall develop and publish practical guidance on legal considerations related to agency use of electronic filing and record keeping.

(e) General Services Administration.

The General Services Administration shall support agencies' implementation of electronic signatures and related electronic service delivery.

Part II. Paperwork Elimination Through the Use of Electronic Signatures and Electronic Record Keeping

This part provides Federal managers with basic information to assist in planning for an orderly and efficient transition to electronic government. Agencies should begin their planning promptly to ensure compliance with the timetable in the GPEA.

Section 1. Introduction and Background

a. As required by the Government Paperwork Elimination Act (GPEA), this Part provides guidance for agencies to use in deciding whether to use electronic signature technology for an application, which electronic signature technology may be most appropriate, and how to minimize the risk of fraud, error, or misuse when implementing an electronic signature technology to authenticate electronic transactions. These procedures are consistent with the requirement of the Paperwork Reduction Act of 1995 (PRA) that agencies shall ''consistent with the Computer Security Act of 1987 (CSA)(40 U.S.C. 759 note), identify and afford security protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of an agency.'' 44 U.S.C. 3506(g)(3).

b. As the GPEA, PRA, and CSA recognize, the goal of information security is to protect the integrity of electronic records and transactions. Different security approaches offer varying levels of assurance in an electronic environment. Among these approaches (in an ascending level of assurance) are (1) the so-called ''shared secrets'' methods, e.g., personal identification numbers or passwords, (2) digitized signatures or biometric means of identification such as fingerprints or retinal patterns and voice recognition,

and (3) digital signatures. Combinations of approaches (e.g., digital signatures with biometrics) are also possible and may provide even higher levels of assurance. Deciding which to use in an application depends upon the risks associated with the loss, misuse or compromise of the information compared to the cost and effort associated with deploying and managing the increasingly secure methods to mitigate those risks. Agencies must strike a balance, recognizing that achieving absolute security is likely to be in most cases highly improbable and prohibitively expensive.

Section 2. What Is an ''Electronic Signature?''

a. The GPEA defines ''electronic signature'' as follows:

> A method of signing an electronic message that—
> (A) Identifies and authenticates a particular person as the source of the electronic message; and
> (B) Indicates such person's approval of the information contained in the electronic message. (GPEA, section 1709(1)).

This definition should be interpreted by reference to accepted legal definitions of signatures. The term ''signature'' has long been understood as including ''any symbol executed or adopted by a party with present intention to authenticate a writing.'' (Uniform Commercial Code, 1–201(39)(1970)). These flexible definitions permit the use of different electronic signature technologies, such as digital signatures, digitized signatures or biometrics, discussed below. For this reason, while it is the case that, for historical reasons, the Federal Rules of Evidence are tailored to the admissibility of paper-based evidence, the Rules of Evidence have no bias against electronic evidence.

b. In enacting the GPEA, Congress addressed the legal effect and validity of electronic signatures or other electronic authentication:

> Electronic records submitted or maintained in accordance with procedures developed under this title, or electronic signatures or other forms of electronic authentication used in accordance with such procedures, shall not be denied legal effect, validity, or enforceability because such records are in electronic form. (GPEA, section 1707).

Section 3. Risk Factors To Consider In Planning and Implementing an Electronic Signature or Record Keeping System

Electronic signature technologies can offer degrees of confidence in authenticating identity greater even than the presence of a handwritten signature. These digital tools should be used to control risks in a cost-effective manner. In determining whether an electronic signature is sufficiently reliable for a particular purpose, agencies should consider the relationships between the parties, the value of the transaction, and the likely need for accessible, persuasive information regarding the transaction at some later date. Once these factors are considered separately, an agency should consider them together to evaluate its sensitivity to risk for a particular process.

a. *The relationship between the parties.* Agency transactions fall into five general categories, each of which may be vulnerable to different security risks:

(1) Intra-agency transactions (i.e., those which remain within the same Federal agency).

(2) Inter-agency transactions (i.e., those between Federal agencies).

(3) Transactions between a Federal agency and state or local government agencies.

(4) Transactions between a Federal agency and a private organization—contractor, university, non-profit organization, or other entity.

(5) Transactions between a Federal agency and a member of the general public.

Inter- or intra-governmental transactions of a relatively routine nature will generally entail little risk of a trading partner later repudiating the transaction, and almost no risk of the trading partner committing fraud. Similarly, transactions between a regulatory agency and a publicly traded corporation or other known entity regulated by that agency bear a relatively low risk of repudiation or fraud. Risk also tends to be relatively low in cases where there is an ongoing relationship between the parties. On the other hand, a one-time transaction between a person and an agency, which has legal or financial implications, bears the highest risk. In all cases, the relative value of the transaction needs to be considered.

b. *The value of the transaction.* Agency transactions fall into five general categories, each of which may be vulnerable to different security risks:

(1) Transactions involving the transfer of funds.

(2) Transactions where the parties commit to actions or contracts that may give rise to financial or legal liability.

(3) Transactions involving information protected under the Privacy Act or other agency-specific statutes obliging that access to the information be restricted.

(4) Transactions where the party is fulfilling a legal responsibility which, if not performed, creates a legal liability (criminal or civil).

(5) Transactions where no funds are transferred, no financial or legal liability is involved and no privacy or confidentiality issues are involved (electronic signatures are least necessary in these transactions and should not be used unless specifically required by law or regulation).

c. *The likely need for accessible, persuasive information regarding the transaction at a later point.* Agency transactions fall into five general categories:

(1) Transactions where the information generated will never be needed again.

(2) Transactions where the information generated may later be subject to audit.

(3) Transactions where the information generated may later be subject to dispute by one of the parties (or alleged parties) to the transaction.

(4) Transactions where the information generated may later be subject to dispute by a non-party to the transaction.

(5) Transactions where the information generated may later be needed as proof in court.

d. *Synthesizing the Risk Factors.*

(1) To evaluate the suitability of electronic signature alternatives for a particular application, the agency needs to perform a qualitative risk analysis and should then determine the particular technologies and management controls best suited to minimizing the risk to an acceptable level while maximizing the benefits to the parties involved.

(2) Risk analyses must recognize that no signature alternative is totally reliable and secure. Every method of signature, whether electronic or paper, can be compromised to some degree with enough technology or due to poor security procedures or practices. In estimating the cost of any system, agencies should include costs associated with hardware, software, administration and support of the system, both short-term and long-term. If it would be extremely expensive to set up a very secure system, but past experience with fraud risks and a careful analysis of those risks shows that exposure is low, a less expensive system that deters the majority of fraud is probably warranted. However, in making this tradeoff, agencies should: (a) Evaluate whether the security elements of a less expensive system can be disproportionately exploited resulting in greater exposure to fraud than would be expected in

comparable non-automated systems; and (b) consider management and other non-technical process controls which could reduce those risks.

(3) A qualitative risk analysis also should recognize that all risks and benefits are not quantifiable. While some transactions can be assigned a definite monetary value that may be placed at risk, many cannot. For example, the value of deterring fraud cannot generally be quantified. Should an agency conclude that a new automated system is less secure than an old, paper-based system, attempts to commit fraud or to repudiate transactions may increase. On the benefit side, it is not always possible to assign a dollar value to the increased efficiency that an agency experiences when it automates a labor-intensive process, although agencies should attempt to make this estimation whenever feasible. Usually, it is not possible to quantify in monetary terms attitudes such as increased customer satisfaction and willingness to cooperate with an agency, which are engendered by the transition from onerous paper processes to user-friendly electronic processes.

(4) One advantage of electronic authentication is that an agency may strengthen the signature validation by incorporating electronic links between the user and preexisting data about that user in the agency's records. The IRS has successfully adopted this approach in its TeleFile program, which enables selected taxpayers to file 1040EZs with a touch-tone phone. Taxpayers get Customer Service Numbers (CSNs, i.e., PINs) that they then use to sign their returns and which help to validate their identities to the agency. Even though a CSN is not unique to an individual taxpayer (since it is only five digits long), the IRS authenticates the filer by using other identifying factors, such as the taxpayer's date of birth, taxpayer identification number, and by using additional procedures. This approach is not used over the Internet. Rather, it occurs in short-term connections over telephone lines, an environment where it is comparatively difficult for malefactors to eavesdrop and to steal information or to substitute false information for fraudulent purposes.

(5) The Computer Security Act places on agency managers the responsibility to select an appropriate combination of technologies and practices to minimize risk cost-effectively while maximizing benefits to the agency and to its customers. These decisions, however qualitative, should be documented for later review and adjustment.

Section 4. Privacy and Disclosure

Section 1708 of the GPEA limits the use of information collected in electronic signature services for communications with a Federal agency. It directs agencies and their staff and contractor personnel not to such use information for any purpose other than for facilitating the communication. Exceptions exist if the person (or entity) who is the subject of the information provides affirmative consent to the additional use of the information, or if such additional use is otherwise provided by law. Accordingly, agencies should follow several privacy tenets:

a. Electronic authentication should only be required where needed. Many transactions do not need, and should not require, detailed information about the individual.

b. When electronic authentication is required for a transaction, do not collect more information from the user than is required for the application.

c. Users should be able to decide the scope of their electronic means of authentication. In other words, if a user wants a certain mechanism for authentication to work only with a single agency or for a single type of transaction, the user's desires should be honored if practicable. Conversely, if the user wishes to have the authentication work with multiple agencies or for multiple types of transactions, that should also be permitted consistent with how the agency employs such means of authentication and with relevant statute and regulation.

d. 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 under the Privacy Act, the Computer Security Act, and any agency-specific statutes mandating the protection of such information.

Section 5. Overview of Current Electronic Signature Technologies

This section addresses two categories of security: (1) Non-cryptographic methods of authenticating identity; and (2) cryptographic control methods. The non-cryptographic approach relies solely on an identification and authentication mechanism linked to a specific software application. Cryptographic controls can be used for multiple applications, if properly managed, and encompass authentication and encryption services. A highly secure implementation may combine both categories of technologies. The spectrum of electronic signature technologies currently available is described below.

a. Non-Cryptographic Methods of Authenticating Identity

(1) *Personal Identification Number (PIN) or password:* A user accessing an agency's electronic application is requested to enter a ''shared secret'' (called ''shared'' because it is known both to the user and to the system), such as a password or PIN. When the user of a system enters her name, she also enters a password or PIN. The system checks that password or PIN as a shared secret to ''authenticate'' the user. If the authentication process is performed over an open network such as the Internet, it is usually essential that at least the shared secret be encrypted; this can be accomplished through the technology called ''Secure Sockets Layer'' currently built into almost all popular Web browsers, in a fashion that is transparent to the end user.

(2) *Smart Card:* A smart card is a plastic card the size of a credit card which contains an embedded chip that can generate, store, and/or process data. It can be used to facilitate various authentication technologies. A user inserts the smart card into a card reader device attached to a microcomputer or network input device. In the computer, information from the card's chip is read by security software only when the user enters a PIN, password, or biometric identifier. This method provides greater security than use of a PIN alone, because a user must have both (a) physical possession of the smart card and (b) knowledge of the PIN. Good security requires that the smart card and the PIN never be kept together. Note that the PIN, password or biometric identifier in this case is a secret shared between the user and the smart card, not between the user and a local or remote computer.

(3) *Digitized Signature:* A digitized signature is a graphical image of a handwritten signature. Some applications require a user 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 is compared with a stored copy of the graphical image of the handwritten signature. If special software considers both images comparable, the signature is considered valid. This application of technology shares the same security issues as those using the PIN or password approach, because the digitized signature is another form of shared secret known both to the user and to the system. The digitized signature is more reliable for

authentication than a password or PIN because there is a biometric component to the creation of the image of the handwritten signature. Forging a digitized signature can be more difficult than forging a paper signature to the extent that the technology digitally compares the submitted signature image with the known signature image, and is better than the human eye. Another element in a digitized signature which helps make it unique is measuring how each stroke is made—its duration or pen pressure, for example. This information can also be compared to a reference value. As with all shared secret techniques, compromise of a digitized signature image file could pose a security risk to users.

(4) *Biometrics:* Individuals have unique physical characteristics that can be converted into digital form and then interpreted by a computer. Among these are voice patterns (where an individual's spoken words are converted into a special electronic representation), fingerprints, and the blood vessel patterns present on the retina (or rear) of one or both eyes. 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. If the test pattern and the previously stored patterns are sufficiently close (to a degree which is usually selectable by the authenticating application), the authentication will be accepted by the software, and the transaction allowed to proceed. Biometric applications can provide very high levels of authentication especially when the identifier is obtained in the presence of a third party (making spoofing difficult), but as with any shared secret, if the digital form is compromised, impersonation becomes a serious risk. Thus, just like PINs, such information should not be sent over open networks unless it is encrypted. Moreover, measurement and recording of a physical characteristic can raise privacy concerns.

b. Cryptographic Control

Creating electronic signatures may involve the use of cryptography in two ways: symmetric (or shared private key) cryptography, or asymmetric (public key/private key) cryptography. The latter is used in producing digital signatures, discussed further below.

(1) *Shared Private Key Cryptography.* In shared private key (symmetric) approaches, the user signs a document and verifies the signature using a single key (consisting of a long string of zeros and ones) that is not publicly known, or is secret. Since the same key does these two functions, it must be transferred from the signer to the recipient of the message. This situation can undermine confidence in the authentication of the user's identity because the private key is shared between sender and recipient and therefore is no longer unique to one person. Since the private key is shared between the sender and possibly many recipients, it is really not ''private'' to the sender and hence has lesser value as an authentication mechanism. This approach offers no additional cryptographic strength over digital signatures (see below). Further, digital signatures avoid the need for the shared secret.

(2) *Public/Private Key (Asymmetric) Cryptography—Digital Signatures.* (a) 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 private key cannot be deduced from the public key. In practice, the public key is made part of a ''digital certificate,'' which is a specialized electronic document digitally signed by the issuer of the certificate, binding the identity of the individual to his or her private key in an unalterable fashion.

(b) A ''digital signature'' is created when the owner of a private signing key uses that key to create a unique mark (called a ''signed hash'') on an electronic document or file. The recipient employs the owner's public key to validate the authenticity of the attached private key. This process also verifies that the document was not altered. Since the two keys are mathematically linked, they are unique: only one public key will validate signatures made using its corresponding private key. Moreover, if the private key has been properly protected from compromise or loss, the signature is unique to the individual who owns it, that is, the owner is bound by the signature. One concern in relatively high-risk transactions is that the private key owner could feign loss to repudiate a transaction. This concern can be mitigated by encoding the private key onto a smart card or an equivalent device, and by using a biometric mechanism (rather than a PIN or password) as the shared secret between the user and the smart card for unlocking the private key to effect a signature. It can also be addressed by agencies establishing clear procedures for a particular implementation, so that all parties know what the obligations, risks and consequences are.

The reliability of the digital signature is directly proportional to the degree of confidence one has in the link between the owner's identity and the digital certificate, how well the owner has protected the private key from compromise or loss, and to the cryptographic strength of the methodology used to generate the key pair. Further information on digital signatures can be found in Access with Trust (http://gits-sec.treas.gov), a report published by OMB and NPR.

c. Technical Considerations of the Various Technologies

(1) While generally the most certain method for assuring identity electronically, use of digital signatures requires agencies to develop a series of policies and documents which provide the important underlying framework of trust and which facilitate the evaluation of risk. The framework identifies how well the signer's identity is bound to his or her public key in a digital certificate (identity proofing); whether the private key is placed on a highly secure hardware token or is encapsulated in software only; and how difficult it is for a malefactor to deduce using cryptographic methods the private key (the cryptographic strength of the key-generating algorithm).

(2) By themselves, digitized (not digital) signatures, PINs and biometric identifiers do not directly bind identity to the contents of a document. For them to do so, they must be used in conjunction with some other mechanism. Biometric identifiers such as retinal patterns used in conjunction with digital signatures can offer far greater proof of identify than pen and ink signatures.

(3) While not as robust as biometric identifiers and digital signatures, PINs have the decided advantage of proven customer and citizen acceptance, as evidenced by the universal use of PINs for automated teller machine transactions. Such transactions, however, typically occur over proprietary networks rather than open networks like the Internet, where eavesdropping on transactions is much easier, unless the messages are encrypted.

(4) It is important to remember that technical factors are but one aspect to be considered when an agency plans to implement electronic signature-based applications. Other important aspects are considered in the following sections.

Section 6. Agency Implementation of Electronic Signature and Authentication

After the agency has conducted the risk analysis and identified an appropriate electronic signature or other electronic authentication, the agency will then proceed to implement this decision. In doing so, agencies should consider the following:

a. *Develop a regulatory or policy scheme.* Agencies should consider whether their programmatic regulations or policies support the use and enforceability of electronic signature alternatives to handwritten signatures. By clearly informing the regulated community that electronic signatures and records will be acceptable and used for enforcement purposes, their legal standing is enhanced. Several agencies have already promulgated policies and regulations making this clear, and a number are developing them:

Securities and Exchange Commission (17 CFR Part 232), electronic regulatory filings; Environmental Protection Agency (55 FR 31,030 (1990)), policy on electronic reporting;

Food and Drug Administration (21 CFR Part 11), electronic signatures and records; Internal Revenue Service (Treasury Reg. 301.6061–1), signature alternatives for tax filings;

Federal Acquisition Regulation (41 CFR Parts 2 and 4), electronic contracts; General Services Acquisition Regulation (48 CFR Part 552.216–73), electronic orders; Federal Property Management Regulations (41 CFR Part 101–41), electronic bills of lading.

When specifying the requirements for using electronic record keeping by regulated entities (particularly the maintenance of electronic forms pertaining to employees by employers), agencies should consider the ''Performance Guideline for the Legal Acceptance of Records Produced by Information Technology Systems,'' developed by the Association for Information and Image Management (ANSI AIIM TR31). This document provides suggestions for maximizing the likelihood that electronically filed and stored documents will be accorded full legal recognition. If an agency chooses to use digital signatures, a regulation may specify that each individual will be issued a unique digital signature certificate to use, agree to keep the private key confidential, and agree to accept responsibility for anything that is submitted using that key, or other conditions under which the agency will accept electronic submissions using it.

b. *Use a mutually-understood, signed agreement between the person or entity submitting the electronically-signed information and the receiving Federal agency.*

(1) As a matter of efficiency, contractual arrangements with large numbers of trading partners would be best accomplished by setting forth an agency's terms and conditions in a regulation. Arrangements with smaller numbers of trading partners may lend themselves to one or more agreements, using a document referred to as a ''terms and conditions'' agreement. These agreements can ensure that all conditions of submission and receipt of data electronically are known and understood by the submitting parties. This is particularly the case where terms and conditions are not spelled out in agency programmatic regulations.

(2) It is also important to establish that the user of the digital signature or PIN/password is fully aware of what he or she is signing at the time of signature. This can be ensured by programming appropriate ceremonial banners that alert the individual of the gravity of the action into the software application. The presence of such banners can later be used to demonstrate to a court that the user was fully informed of and aware of what he or she was signing.

c. *Minimize the likelihood of repudiation.* Agencies should develop well-documented and established mechanisms and procedures to tie transaction in a legally binding way to an individual. The integrity of even the most secure digital signature rests on the continuing confidentiality of the private key, for example. Similarly, in the case of electronic signatures based on the use of PINs, the integrity of the transaction depends on the user not disclosing the PIN. If a defendant is later charged with a crime based on an electronically signed document, he or she would have every incentive to show a lack of control over (or loss of) the private key or PIN. Indeed, if that defendant plans to commit fraud, he or she may intentionally compromise the secrecy of the key or PIN, so that the government would later be unable to link him or her to the electronic transaction.

Thus, 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. One way to mitigate this risk is to require that private keys be encoded on hardware tokens, making possession of the token a critical requirement. Another way to guard against fraud is to include other identifying data in the transaction that links the key or PIN to the individual, preferably something not readily available to others.

d. *Access to the electronic data, after receipt, needs to be carefully controlled yet available in a meaningful and timely fashion.* Security measures should be in place that ensure that no one is able to alter a transaction, or substitute something in its place, once it has been received by the agency. Thus, the receiving agency needs to take prudent steps to control access to the electronic transaction through such methods as limiting access to the computer database containing the transaction, and performing processing with the data using copies of the transaction rather than the original. Moreover, the information may be needed for audits, disputes, or court cases many years after the transaction itself took place. Agencies should make plans for storing data, and providing meaningful and timely access to it for as long as such access will be necessary.

e. *Ensure the ''Chain of Custody.''* Electronic audit trails must provide a chain of custody for the secure electronic transaction that identifies sending location, sending entity, date and time stamp of receipt, and other measures used to ensure the integrity of the document. These trails must be sufficiently complete and reliable to validate the integrity of the transaction and to prove that, (a) the connection between the submitter and the receiving agency has not been tampered with, and (b) how the document was controlled upon receipt.

f. *Provide an acknowledgment of receipt.* The agency's system for receiving electronic transactions may be required by statute to have a mechanism for acknowledging receipt of transactions received, and acknowledging confirmation of transactions sent, with specific indication of the party with whom the agency is dealing.

g. *Obtain legal counsel during the design of the system.* Collection and use of electronic data may raise legal issues, particularly if it is information that bears on the legality of the process or that may eventually be needed for proof in court.

Section 7. Summary of the Procedures and Checklist

To summarize the process which agencies should employ to evaluate authentication mechanisms (electronic signatures) for electronic transactions and documents, the following steps apply:

1. Examine the current business process that is being converted to employ electronic documents or

transactions, identifying the existing risks associated with fraud, error or misuse, as well as customer needs and demands.

2. 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.

3. Identify the benefits that accrue from the use of electronic transactions or documents.

4. Consult with counsel about any 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 cost and risk on the one hand, and benefits 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 evaluation and audit.

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. Determine if regulations or policies are adequate to support electronic transactions and record keeping, or if ''terms and conditions'' agreements are appropriate for the particular application.

9. Develop plans for seeking the 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.

10. Integrate these plans into the agency's strategic IT planning and regular reporting to OMB.

11. Perform periodic review and re-evaluation, as appropriate.

[FR Doc. 99–5409 Filed 3–4–99; 8:45 am]

BILLING CODE 3110–01–U