GAO

United States
General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

B-283132

July 2, 1999

Information Policy and Technology Branch
Office of Information and Regulatory Affairs
Office of Management and Budget

Subject: Information Technology: Comments on Proposed OMB Guidance for Implementing the Government Paperwork Elimination Act

This letter is in response to your request for comments on the Proposed OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act (GPEA). We support the stated goals of the draft guidance and appreciate the difficulties in developing practicable guidance for agency managers to implement these goals.

We concur with your approach of determining the internal controls based on a risk assessment. However, we believe that additional guidance is needed to help the agencies determine the risk assessment methodology. Specifically, we suggest that you (1) require a quantitative as well as a qualitative risk analysis as part of any risk assessment process and (2) provide additional information to help agencies properly consider the implications that historic weaknesses in agency internal controls have had on data integrity during the risk assessment process.

The enclosures to this letter provide our detailed comments and suggestions for improving the proposed guidelines. Enclosure 1 provides specific comments and suggestions on risk assessments, enclosure 2 provides specific comments and suggestions on individual sections, and enclosure 3 contains suggestions for improving the implementation guidance by defining certain key terms.

If you have any questions or need additional information, I can be reached at (202) 512-6415.

Keith A. Rhodes
Director, Computers and
Information Technology Assessment

Enclosures (3)

167412

Better Guidance Needed for Risk Assessments

The sections discussing the risk assessments would benefit by clarifying the risk assessment definition, discussing the effects of breakdowns in general ADP controls on data integrity, and providing a framework on how risk assessments should be prepared. These are discussed below.

Risk Assessment Definition Needs Clarification

Part I, Section 2.c., states that a risk assessment is required and is used to develop baselines and verifiable performance measures that track the agency's mission, strategic plans, and tactical plans. Normally, a risk assessment is used to determine the risks associated with a given project, the probability that a given risk will occur, and the impact of those risks that do materialize. This analysis is then used to develop a risk management plan which identifies the techniques, if any, that will be used to mitigate each risk. Normally other documents in the project life cycle are used to (1) map the project to an agency's mission, strategic plans, and tactical plans and (2) specify the baselines and performance measures that will be used to evaluate the program.

We would suggest revising this section to state that a quantitative and qualitative risk assessment must be performed[1] on the proposed electronic records project and include (1) the risks associated with the project, (2) the probability, if available, of the risk materializing, and (3) the potential impact if a risk does materialize. This section should also state that once the risk assessment is completed, a risk management plan should be prepared and properly maintained to manage the risks that were identified.

Risks Associated With Breakdowns in General ADP Controls

Part II, Section 6.d., discusses the need to carefully control the access to electronic data to ensure that no one can alter the received data. It also notes that the data may be needed many years after the transaction itself took place. Theoretically, it would be possible to maintain the necessary data integrity using any of the electronic signature techniques identified in section 5 if properly implemented and, depending on the electronic signature technique, accompanied by the appropriate general computer security controls. However, in the electronic world, because of the difficulty in detecting unauthorized modifications to electronic data,[2] the only practical way that current technology can ensure that no one will be able to alter an electronic transaction, or substitute something in its place, without detection is to require the use of self-authenticating electronic signature techniques. Self-authenticating electronic signature techniques link the data to the electronic signature in such a manner that if the data is altered, the signature is invalidated during the electronic signature verification process.

We suggest that OMB, for the present, require the use of self-authenticating electronic signature techniques when the risk assessment identifies the need for them. Examples of technologies, properly implemented, that can conceptually produce self-authenticating electronic signatures

[1] This is consistent with An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12.

[2] A paper document allows certain forensic tests, such as chemical analysis, to determine if an alteration has occurred. These tests cannot be duplicated on the electronic data unless the data is linked to the signature in such a manner that a change to the data invalidates the signature.

include voice prints, symmetric key cryptographic systems using a technique commonly referred to as key notarization, and public/private key cryptographic systems.

We believe that the guidance, as currently drafted, does not provide sufficient detail for agencies to understand and evaluate the risks associated with trying to securely maintain electronic data when the electronic signature is not directly linked to the data. As noted in our recent update on the high-risk issues facing the federal government,[3] our reviews of computer security across the federal government have disclosed disturbing weaknesses that make it easier for individuals and groups to intrude into inadequately protected systems and use such access to obtain sensitive information, commit fraud, or disrupt operations. Examples include the following:

- In May 1998, we reported that the Department of State's information systems and the sensitive data they maintain were vulnerable to access, change, disclosure, and disruption by unauthorized individuals.[4] In addition to recommendations to correct individual deficiencies, we recommended that the agency strengthen its management structures for planning and implementing its information security program.

- In September 1998, we reported that weaknesses at the Department of Veterans Affairs placed critical operations, such as healthcare delivery, benefit payments, and life insurance services, at risk of misuse and disruption. We recommended that the department's Chief Information Officer correct all identified weaknesses and implement a comprehensive computer security planning and management program.[5]

- In September 1998, we reported that our review of two cases of Air Force vendor payment fraud disclosed that computer security weaknesses continued to make the Air Force vulnerable to such incidents. We recommended strengthening operating system controls and assessing the need for stronger controls over user identifications and passwords.[6]

- For the last 7 years, the USDA Inspector General has reported serious computer control weaknesses at the National Finance Center, which annually makes over $21 billion in payroll disbursements to about 434,000 employees and about $15 billion in other payments. The Inspector General reported that the center had not ensured that (1) systems security adequately prevented misuse or unauthorized modifications, (2) access to data was needed or appropriate, and (3) modifications made to software programs were properly authorized and tested. USDA has actions planned to correct these serious weaknesses.

The practical implication of these weaknesses is that although the agencies may strive to ensure electronic data integrity through system controls, they have failed to achieve the kind of assurance that the draft guidance expects. Although the nature of agency operations and the related risk vary, there are striking similarities in the control weaknesses reported. The most widely reported weaknesses have been

[3] High-Risk Series: An Update (GAO/HR-99-1, January 1999).

[4] Computer Security: Pervasive, Serious Weaknesses Jeopardize State Department Operations (GAO/AIMD-98-145, May 18, 1998).

[5] VA Information Systems: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure (GAO/AIMD-98-175, September 23, 1998).

[6] Financial Management: Improvements Needed in Air Force Vendor Payment Systems and Controls (GAO/AIMD-98-274, September 28, 1998).

- poor control over access to sensitive data and systems, such as providing overly broad access privileges to very large user groups, allowing shared passwords and user accounts, and inadequate monitoring of user's activities;

- mitigating and recovering from unplanned interruptions in computer service;

- inadequately segregating duties to help ensure that people do not conduct unauthorized actions without detection; and

- not preventing unauthorized software from being implemented.

We also noted in our report that security risks to government computer systems are significant and growing and that agencies have not responded to audit findings with enough attention to the systemic problems. The threats to data integrity caused by these weaknesses are hard to quantify, and agencies may not even know if they have been attacked.

In 1996 we testified that the Department of Defense's computer systems are being attacked every day. Although Defense does not know exactly how often hackers try to break into its computers, the Defense Information Systems Agency (DISA) estimated that as many as 250,000 attacks may have occurred in 1995. (Currently, DOD estimates that about 500,000 attacks occur annually.) An equally worrisome finding noted in our testimony was that DISA conducted internal tests to help it quantify system vulnerabilities and found that it could successfully penetrate Defense systems 65 percent of the time. Not all hacker attacks result in actual intrusions into computer systems; some are attempts to obtain information on systems in preparation for future attacks, while others are made by the curious or those who wish to challenge the Department's computer defenses.[7]

Some attacks on DOD's computers have had very serious results. Hackers have stolen and destroyed sensitive data and software. They have installed "backdoors" into computer systems which allow them to surreptitiously regain entry into sensitive Defense systems. They have "crashed" entire systems and networks, denying computer service to authorized users and preventing Defense personnel from performing their duties. We pointed out in the testimony that an attack on the Air Force's laboratory in Rome, New York, demonstrated how easy it was for hackers to gain access to our nation's most important and advanced research and how difficult it is to value and apprise the information contained in a system.

Although linking electronic signatures to the data contained in government systems using self authenticating electronic signature techniques does little to protect the network against hacker attacks that cause a loss of data or services, the linking is a very good technique to help ensure that system data integrity has not been compromised or at least identify the records that were changed. For example, if an unauthorized user obtains access to an electronic report that does not use self-authenticating electronic signature techniques and changes the data, it is very difficult to determine if an alteration occurred. However, if self-authenticating electronic signature techniques are properly implemented and used, then by simply validating the electronic signature, the agency can identify if any records have been altered. In other words, electronic signature techniques that link the electronic signature to the data in such a manner that if the data are changed, the signature is invalidated during the signature verification process, can help mitigate the weaknesses in the general computer controls discussed above that plague many federal computer systems and compromise data integrity.

[7] Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/T-AIMD-96-92, May 22, 1996).

Implementation Guidance Needs to Provide a Framework to Evaluate Risks to Data Integrity

Part II, Section 3., outlines three categories of risk factors and how to synthesize them when planning and implementing electronic signature or recordkeeping systems. However, this section does little to explain the logical steps necessary to assess the risk associated with a given system and ensure that the system is available, reliable, survivable, and secure. We believe that it would be useful to revise this section and provide the framework of analysis that should be used to build the systems envisioned by this guidance. Examples of areas that should be revised include the following:

- The introduction states that "[e]lectronic signature technologies can offer degrees of confidence in authenticating identity greater even than the presence of a handwritten signature." Although this is true, the draft does not provide the necessary information to properly evaluate the statement. It does not state that because electronic records have risks, such as modifying data from a remote location, that are not present in their paper-based counterparts, such techniques are necessary to provide the same overall assurance that the data integrity has been maintained.

- The categories in Part II, Section 3.a., are prefaced with the statement that each category is vulnerable to different security risks. However, in the material that follows these categories, it appears that although the risk factors differ, all but one transaction type (transactions between a federal agency and member of the general public) should be considered low risk. The support that was used to make the risk assumptions in this section is unclear. For example, the draft guidance states that "transactions between a regulatory agency and a publicly traded corporation or other known entity bear a relatively low risk of repudiation or fraud."

- Part II, Sections 3.b. and c., outline five categories each and state that each category is vulnerable to different security risks. However, these sections do not provide any guidance on how an agency should evaluate the risks associated with these categories or the types of risks associated with each.

- Part II, Section 3.d.1., states that the agency should perform a qualitative risk analysis in order to determine the electronic signature technologies and management controls that are best suited to minimizing the risk to an acceptable level while maximizing the benefits to both parties involved. While qualitative analysis is important to making an informed decision, quantitative analysis is also an important indicator since it produces an evaluation that can be used by third parties, such as OMB and the Congress, using fact-based methodologies. If an agency does not have enough information to perform a quantitative analysis, then it does not have enough information to evaluate the reasonableness of the qualitative analysis. Also, we are concerned that agencies may not provide the rigor necessary to evaluate the risks associated with the project if a quantitative risk analysis is not performed.

- Part II, Section 3.d.2., discusses using the past history of fraud risk and states that careful analysis of those risks should be used to help determine the electronic signature alternative that is needed. History has shown that risks associated with automated systems may vary significantly from those found in the paper-based counterparts. Therefore, effective risk analysis programs (1) identify the risks associated with the system being developed, (2) quantify the probability of the risk materializing, and (3) quantify the effect of the risk if it does materialize.

- The opening statement in Part II, Section 3.d.4., states that electronic authentication may strengthen signature validation. It is unclear how electronic authentication can strengthen the signature validation process. Rather, it appears this example demonstrates how the electronic signature is generated by using numerous items to help authenticate the signer.

Although it is unreasonable to expect that all risks associated with a given system can be identified and quantified before a system is implemented, it is important to have an effective methodology that identifies the unique risks associated with a given approach.

We suggest that this section be revised to state the framework that agencies should use to determine controls needed to ensure that the system is available, reliable, survivable, and secure. Adopting the following three-step approach would provide practical guidance, while allowing agencies a great deal of flexibility to develop systems that meet their business needs.

- Prepare a quantitative and qualitative risk assessment based on the system requirements that (1) identifies the risks associated with the system being developed, (2) quantifies the probability of the risk materializing, and (3) quantifies the effect of the risk if it does materialize.

- Develop and maintain an effective risk management plan that identifies the techniques, if any, that will be used to mitigate the identified risk.

- Ensure that the control techniques identified in the risk management plan are properly implemented. An agency could assess its controls annually as a part of its Federal Managers' Financial Integrity Act review process.

It would be very useful to have OMB request an agency, such as NIST, that has computer security expertise to prepare guidance for agencies to use in preparing the risk assessment and risk management plan. For example, a list of standard risks that should be considered in the risk assessment process and techniques that can be used to mitigate those risks would reduce the amount of effort each agency would need to spend to develop its risk documents. Although the agencies would need to ensure that the unique risks associated with a given project were identified, they would not have to spend time "reinventing the wheel" to ascertain the standard risks and identify acceptable techniques to mitigate them. Rather, agency officials could make a decision on whether a standard risk was present in their system and focus their efforts on determining whether (1) it needed to be mitigated and (2) the standard control techniques identified in the standard guidance are adequate and/or any additional controls may be needed.

Specific Comments on Individual Sections

In reviewing the draft guidance, we also noted areas that could use additional clarification or could be added to improve the usefulness of the document. These include

- clarifying the information in the section that discusses electronic signature technologies,
- discussing the importance of general computer controls and the impact weaknesses in these areas can have on data reliability,
- providing additional guidance relating to audit trails,
- involving the Inspectors General in system design and development efforts,
- improving the summary of procedures checklist, and
- including a discussion on the unique factors associated with federal government automation efforts that should be considered when agencies automate their systems.

Our comments and suggested changes are discussed below.

Clarification Needed in Section Discussing Electronic Signature Technologies

The section heading in Part II, Section 5., states that it contains an overview of electronic signature technologies. This section would benefit from a lead-in that discusses the risks associated with electronic signature techniques which do not produce self-authenticating electronic signatures to help agencies develop the risk assessments called for in other sections of the draft guidance. One risk that appears to apply to all of these technologies is the risk of capturing the authenticating information and resubmitting it to gain unauthorized access. In some cases, the material provided in this section does not make this risk obvious. Examples include the following:

- The discussion on personal identification numbers and passwords states that the authentication process should be encrypted when transmitted over the Internet and this can be accomplished using a technology called the "Secure Sockets Layer." However, this section does not discuss the risks to the computer server that provides these services and the types of controls that are needed to ensure that the services provide the expected level of assurance.
- The section states that forging a digitized signature is more difficult than forging a paper signature since, during the verification process, the digitized signature is compared to a stored image with a technology that is better than the human eye. It also states that the creation of the image helps make it unique because the technology measures how each stroke is made. However, the discussion does not state that if this technology is to provide this degree of assurance, a trusted path[7] must exist between the device capturing the digitized signature and the device authenticating it. A statement that the transmission of digitized (not digital) signatures should not be sent over open networks unless they are encrypted would also be a useful addition. The section on biometrics contains this type of statement.

[7] A mechanism by which a person or process can communicate directly between two devices or processes and which can only be activated by the person, process, or module, and cannot be imitated by untrusted software or processes.

In addition, the discussion of several technologies could be enhanced with some additional material. Examples include the following:

- The discussion on symmetric key cryptography in Part II, Section 5.b.1., gives the impression that this technology undermines the confidence of the signature because the same key is used to generate and validate the signature. While this is a valid point, it would be useful to acknowledge that the effects of this can be reduced through the use of key notarization and provide an example of this technology. We would also suggest using the electronic signature system developed by the Corps of Engineers, which we understand is used by over 10,000 employees worldwide, as an example.

- It would be useful to provide additional information in Part II, Section 5.b.2., on the need for certificates in digital signature systems and a clearer explanation of how a digital signature is generated. We would suggest something like the following:

  > "Although the private key cannot be deduced from the public key, anyone can generate the necessary public/private key pair. Therefore, a means is needed to bind an individual's identity to the public key that will be used to validate an individual's digital signature. This binding is normally performed by using a specialized electronic document, commonly referred to as a certificate, which is signed by the issuer and contains the user's public key.
  >
  > "A 'digital signature' is created during a two-step process. The electronic document is first reduced to a value commonly referred to as a message digest. This message digest is developed using a process that ensures that (1) the digest is unique to that message and (2) it is very difficult to generate another message that would generate the same message digest. The system then takes the signer's private key and creates a unique mark (called a 'signed hash' or 'digital signature') on this value.
  >
  > "The recipient of the message takes the message and recomputes the message digest and then, using the signer's public key, verifies the signed hash (digital signature). If these two values agree, then the recipient has reasonable assurance that the document was not altered. Since the private key used to sign the message and the public key used to validate the signature are mathematically linked and unique, only one public key can be used to validate a given signature. Moreover, . . ."

- In Part II, Section 5.b.2., a statement is made that 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 the cryptographic strength of the methodology used to generate the key pair." These are very good points, and additional information would be beneficial to help explain the importance of binding an individual to the public key and protecting the private key from compromise. Furthermore, many agencies may not understand the importance of the last part of the requirement that discusses the methodology used to generate the key pair. Although that methodology is important, other factors are just as important. For example, the algorithm selected for generating and validating digital signatures and ensuring that a given implementation is secure is critical to a secure system.

  It would be useful if the guidance included a discussion of how acceptable electronic signature systems are built upon standards and technology that are recognized by NIST and independent standards organizations such as the American National Standards Institute (ANSI) and the International Organization of Standardization (ISO). The reliance on NIST would appear consistent with the Computer Security Act, which states that NIST has the primary responsibility for developing standards for cost-effective computer security associated with systems processing sensitive but unclassified data. History has shown that standards which have not undergone a rigorous standard-setting process may have unforeseen weaknesses and they may result in proprietary solutions. Therefore, it is critical that the standards have a sound basis before they are eligible for adoption.

Although the draft guidance states that agencies need to perform a risk assessment before adopting any electronic signature solution, it is unclear whether agencies will have enough information to adequately determine the risks associated with a given industry solution. In our experience, most agencies are not in the business of evaluating products for security weaknesses. Rather, they rely on others, such as independent testing organizations, to validate that a given product complies with standards from a recognized standard-setting body to help reduce the risks associated with acquiring products with unforeseen security weaknesses.

Discussion of General Computer Controls and Repudiation Needs Additional Information

Part II, Sections 6.c. and d., discuss data integrity issues and the need to minimize the likelihood of repudiation and the importance of a user not disclosing a personal identification number (PIN) or the cryptographic key used to sign a message. The section also states that if a defendant plans to commit fraud, he or she may intentionally compromise the secrecy of the key or PIN that was used to produce the electronic signature so that the government would later be unable to link the individual to the electronic data. This section needs to be expanded to discuss the importance of considering the system risks that may also affect the government's ability to (1) claim that a defendant maintained sole control over the signature mechanism and (2) protect the government's electronic signature capability for its transactions.

Although Section d. states that the electronic data, after receipt, needs to be carefully controlled, these sections do not discuss the problems that must be addressed when a defendant claims that the system lacks adequate controls to provide the necessary data integrity. As noted elsewhere in our comments, our reviews of computer security across the federal government have disclosed disturbing weaknesses that make it easier for individuals and groups to intrude into inadequately protected systems and use such access to obtain sensitive information, commit fraud, or disrupt operations. It is very possible that a defendant will claim that he or she properly protected the PIN but that because the agency did not have adequate computer security controls, the data were changed after they were submitted by the defendant. While the risk assessment called for in other sections of the draft guidance should address these kinds of issues, it would be useful to highlight them in this section of the guidance and note that they should be specifically addressed in the risk assessment.

Additional Guidance Needed Relating to Audit Trails

The discussion in Part II, Section 6.e., requires that the system ensure the "chain of custody." The material in this section appears to require the use of self-authenticating electronic signatures. Since other sections of the draft guidance do not distinguish between signature techniques, it may be useful to discuss when self-authenticating electronic signatures, rather than other types of electronic signatures, are needed.

Involvement of Auditors Needed During System Development Efforts

Part II, Section 6.g., states that legal counsel should be involved during system design. It is also useful to involve the agency's inspector general in the proposed system development to ensure that adequate audit trails are incorporated into the system and that the quantitative and qualitative risk assessment is properly prepared. Involving the agency's auditors would help agency management gain confidence that the system is complying with the OMB guidance and other pertinent requirements.

Summary of Procedures Checklist Can Be Improved

Part II, Section 7., outlines 11 steps that should be taken to comply with the draft guidance. Organizing these steps according to the logical flow that occurs during a system development effort would assist the agencies in complying with the OMB guidance and other information technology requirements. Examples of weaknesses in the current material include the following.

- Step 1 requires the agency to examine the current business process and identify the existing risks associated with fraud, error, or misuse, as well as customer needs and demands. While identifying the risks associated with the current system may be of some help with the development of the quantitative and qualitative risk assessment, the risks associated with the proposed system need to be identified and assessed in order to perform an adequate assessment. It would appear that the first step should be the development of a concept of operations for the proposed system that describes system characteristics from the user's point of view.[8] The draft guidance also does not discuss the process that will be used to identify the agency's needs.

- Step 2 states that the agency should consider the risks that may arise. As noted earlier, it would be useful to require that a quantitative and qualitative risk assessment be prepared. After the risk assessment is prepared, a risk management plan needs to be developed, implemented, and maintained.

- Step 3 requires the identification of benefits. While this is an important function, it is equally important to identify the costs associated with the proposed system. This analysis should be used to help the agency ensure that the proposed system will meet its information technology investment guidelines.

- Step 4 requires consulting with legal counsel. As noted earlier, the inspector general should also be consulted and these organizations should be involved in developing the concept of operations.

- Step 5 does not clearly explain what is meant by "each electronic signature alternative." As noted elsewhere in our comments, the purpose of a risk assessment is to identify the risks associated with a given approach, and the risk management plan identifies the techniques that will be used to mitigate the risks. The risk management plan should quantify the costs and benefits associated with the techniques that are used to address the risk factors. Adopting this approach would appear to address the objective of step 6.

[8] A concept of operations is used to communicate overall quantitative and qualitative system characteristics to the user, buyer, developer, and other organizational elements. The concept of operations also describes the user organization(s), mission(s), and organizational objectives from an integrated systems point of view. (IEEE Guide for Information Technology – System Definition – Concept of Operations (ConOps) Document, IEEE Std 1362-1998. Institute of Electrical and Electronics Engineers, Inc.)

- Step 8 is very important and should be performed early in the process in order to help the project team define the requirements. If the agency is unable to accomplish the needed changes to regulations or policies, then the system may require substantial changes and no longer meet the agency's information technology investment guidelines. Furthermore, this information is needed to help develop the risk assessment and risk management plans.

Unique Nature of Government Operations Is Not Discussed

Although implementing a system in the federal government is similar to the private sector, some important differences exist. Examples include the following.

- "Customers" of a federal agency may not get to choose whether they would like to report to the federal agency. Generally, customers can choose which private sector company they would like to use. Therefore, the benefits associated with customer choice are not present in federal systems.

- The risk management decisions made by a federal agency need to include risks that are being imposed on the customer. The risks associated with a system from a federal agency point of view may be entirely different than those from the customer's point of view. For example, when the Social Security Administration was considering bringing its Personal Earnings and Benefit Statement online, it generally looked at risks associated with unauthorized individuals gaining access to an individual's records. However, it did not consider the risks to the individual taxpayer of someone using the system to validate critical information that was obtained from a third party. Specifically, an individual who wants to steal another person's identity may try to validate the target individual's date of birth and location that were obtained from a third party. Using the Social Security Administration system, the perpetrator could attempt to gain access. If the access was successful, then the individual would know that he or she had the correct data since these two items were used by the Social Security Administration to help authenticate the user.

- The federal agency may not be able to make a complete conversion to electronic records even if the legacy process is not cost effective. Federal agencies operate in an environment which may require reporting methods that are based on public policy or other non-economic factors. For example, the public comment process may dictate that a given process be continued even if the proposed system is more cost effective.

A section outlining how an agency should address the unique aspects associated with its modernization efforts would be a beneficial addition to the draft guidance.

Key Terms Need to Be Defined

The following sections discuss the draft guidance's use of the terms "cost-benefit analysis" and "electronic authentication."

Cost-Benefit Analysis

Part I, Section 2.d., discusses using the cost-benefit analysis to generate a business case and determine a verifiable return on investment to support decisions regarding overall programmatic direction, investment decisions, and budgetary priorities. It also states that the cost-benefit analysis should be used as a guide to select among the technologies under consideration. However, the purpose of the last sentence–which states that the "effects on the public and its needs and readiness to move to an electronic environment are important considerations"–is unclear.

Normally, an alternatives analysis is used to help decide which technologies should be used to address a given need, and it is prepared after the system requirements have been defined. The completed alternatives analysis provides the recommended approach that is used to further refine the business case. Although cost-benefit techniques are used to develop the alternatives analysis, other information may be equally important. For example, certain alternatives may not be adopted because they do not comply with the agency's system architecture requirements. After an alternative is adopted, a cost-benefit analysis is then developed to assess the overall costs and benefits of the project.

We would suggest revising this section to clearly state that an alternatives analysis must be performed and that before an alternative has been adopted, a cost-benefit analysis for the project be completed to ensure the project meets the agency's information technology investment guidelines. Benefits and costs, such as the value of deterring fraud, which cannot be readily quantified, should also be included.

Electronic Authentication

Part II, Section 1.b., combines techniques which, by their design, provide data integrity (e.g., digital signatures) with techniques that only provide user authentication (e.g., user identification codes and passwords). This presentation approach may lead the reader to believe that given technologies and techniques can be used in isolation to provide a specified level of assurance. For example, Section 1.b. states that digitized signatures and biometric means of identification have a greater degree of assurance than user identification codes and passwords. However, the key to whether one technology will provide a higher degree of assurance than another technology is (1) the risk environment and (2) how well the technology is implemented. For example, transmitting digitally signed unencrypted fingerprints over the Internet as a means to identify a person provides little advantage over using traditional passwords and user identification codes since this authentication mechanism is subject to the same type of risk–capturing the authenticating information and then using it later.[9] This is also true of using digital signatures to identify an individual. If a sound mechanism has not been used to link the actual person to the public key that is used to validate that individual's identity, then the resulting digital signature provides little assurance of an individual's identity.

[9] This should not be interpreted to mean that digitally signed fingerprints cannot be used to provide a reliable means of identifying an individual to a system over an untrusted network. However, each transmission must have some unique information, such as a date/time stamp, to prevent the identification information from being used again at a later date.

Very rarely does one specific technology or control technique provide the necessary assurance. In order to authenticate a user, Federal Information Processing Standard (FIPS) 48 outlines the following three basic methods that are available for establishing the identity of an individual:

- something KNOWN by the individual (e.g., the traditional user identification code and password approach of gaining access to a system),
- something POSSESSED by the individual (e.g., badge and smart cards), and
- something ABOUT the individual (e.g., appearance, fingerprints, and voice).

Normally, it is recommended by the National Institute of Standards and Technology (NIST) that two pieces of information to be used to identify an individual even if the same method is used for both. For example, many systems require the use of user identification codes and passwords to gain access to the system. Even though this approach uses the "something known by the individual" method of identification, using two pieces of information provides a greater degree of assurance than if only one item were used.

Part II, Section 3., gives an example of using at least two pieces of information to identify an individual. It states that although the IRS Customer Service Number (CSN) is not unique to an individual since it is only five digits long, IRS authenticates the filer by using other identifying information, such as the taxpayer identification number. Based on the information provided, it appears that the IRS example uses at least two elements of something the user knows to authenticate the user. In this case, the taxpayer identification number and CSN in combination are unique to the user. This is consistent with the traditional user identification code and password-based approaches to granting access to a system. Although it is possible that two individuals may use the same password, the user identification code and password combination should not be the same because system administrators ensure that each individual has a unique user identification code.

We would suggest revising this section and stating that various technologies, properly implemented, can be used to help provide the necessary integrity over electronic records and transactions and that a number of control techniques are used in combination to provide the necessary level of assurance.

(922271)

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

United States
General Accounting Office
Washington, D.C. 20548-0001