U.S. Department of Justice

LEGAL CONSIDERATIONS IN DESIGNING AND IMPLEMENTING ELECTRONIC PROCESSES:

A GUIDE FOR FEDERAL AGENCIES

NOVEMBER 2000

November 2000

LEGAL CONSIDERATIONS IN DESIGNING AND IMPLEMENTING ELECTRONIC PROCESSES: A GUIDE FOR FEDERAL AGENCIES

U.S. DEPARTMENT OF JUSTICE

EXECUTIVE SUMMARY

Under the Government Paperwork Elimination Act (GPEA), Pub. L. No. 105-277, ''1701-1710 (1998) (codified as 44 U.S.C.A. ' 3504 n. (West Supp. 1999)), Federal Executive agencies are required, by October 21, 2003, to provide for (1) "the option of the electronic maintenance, submission, or disclosure of information, when practicable, as a substitute for paper;" and (2) "the use and acceptance of electronic signatures, when practicable." The Office of Management and Budget (OMB) has developed guidance to assist agencies in implementing GPEA's requirements. "Procedures and Guidance; Implementation of the Government Paperwork Elimination Act," 65 FR 25508, May 2, 2000 ("OMB Guidance"). As part of the OMB Guidance, the Department of Justice is charged with developing, in consultation with federal agencies and OMB, practical guidance on legal considerations related to agency use of electronic filing and recordkeeping. The purpose of this Guide is to identify legal issues that agencies are likely to face in converting to electronic processes and to provide some suggestions on how to address them. Agencies should also consider the significance of the "Electronic Records and Signatures in Global and National Commerce Act" (E-SIGN) (Pub.L. 106-229, § 1, June 30, 2000, 114 Stat. 464, codified at 15 U.S.C. §§ 7001 -- 7006), although a detailed discussion of that statute's impact on the federal agencies is beyond the scope of this Guide.

The rise of electronic commerce offers agencies exciting opportunities to convert -- or redesign -- paper-based processes to electronic ones. While some agencies have experience using electronic processes, others are just beginning to examine the opportunity of electronic processing, or are just beginning to consider electronic processing for more sensitive transactions. In moving to electronic processes, agencies face many important decisions. Among those decisions is one crucial question of interest to the Department of Justice: When an agency converts each type of transaction to an electronic-based process, how should the agency design that process so as to protect its legal rights and minimize legal risks that may compromise the agency's mission? In accordance with the OMB Guidance on GPEA, agency considerations of cost, risk, and benefit, as well as any measures taken to minimize risks, should be commensurate with the level of sensitivity of the transaction. Low-risk information processes may need only minimal safeguards, while high-risk processes may need more. In the context of legal and litigation risks, "low-risk information processes" are those that have a small chance of generating significant liability, financial impact, or litigation that would have a significant effect on the agency.[1]

---

[1] For example, even small transactions that take place in great volume could expose the agency to a large overall risk, even though each particular transaction does not.

The many potential benefits of re-designing (or designing) agency processes to use electronic-based processes are apparent: increased efficiency, accessibility, and reliability. Advances in technology, public expectations, Congress's mandate in the GPEA, and Administration policy all require that agencies of the United States move expeditiously to adopt electronic processes. Some agencies are already seeing benefits from increasing their use of and reliance on electronic recording and transaction systems. These benefits may not be fully realized unless the agency designs its processes with care. This Guide explains the legal issues an agency is likely to face in designing electronic-based processes (Part I), examines four overarching legal issues that should be considered with respect to converting any given type of system or operation (Part II), and discusses general and specific steps agencies should consider in converting to electronic processes (Part III). The reader who already recognizes the legal issues presented by electronic processes and those involved in replacing paper processes with electronic ones may wish to turn first to Part III, which does not depend on the analysis of Parts I and II for an understanding of its suggestions.

In deciding whether and how to convert any given process from paper to an electronic one, agencies should consider at least the following four issues, which are examined in Part II:

- Availability **B** Will the important information regarding a transaction be collected, retained, and accessible whenever needed despite changes to computer hardware or software? How long should the information be kept given legal record-keeping needs? The important transaction information to be collected and accessible typically includes the *content or substance* of the transaction (for example, the text of a contract); the *processing* of the transaction (such as when and from where a communication was sent and when and where it was received); the *identities* of the parties and the specific individuals involved in the transaction; and the *intent* of the parties (such as whether they intended to enter into a binding contract).

- Legal Sufficiency **B** Certain types of transactions must be in "writing" and "signed" in order to be legally enforceable. The law is still developing with respect to whether such requirements will be satisfied by all electronic processes in all circumstances. By using electronic processes that address the issues raised in this Guide, agencies can increase the likelihood that their electronic transactions will meet such legal standards. Federal laws, such as GPEA, address the legal validity and enforceability of electronic records and signatures. GPEA states that: "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." E-SIGN similarly provides that records relating to commercial, financial, or consumer transactions shall not be denied legal effect solely because they are in electronic form or signed by electronic signature. Although Federal activities are usually governed by federal rather

than state law, it is also noteworthy that various state laws, such as versions of the Uniform Electronic Transactions Act (UETA) that are currently being introduced in the states, similarly address the legal validity of electronic records and signatures, including in the formation of a contract. UETA states: "a record or signature may not be denied legal effect or enforceability solely because it is in electronic form. . . [A] contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation."

- Reliability **B** Will electronic records be sufficiently reliable and persuasive to satisfy courts and others who must determine the facts underlying agency actions? Will the electronic records be maintained in such a way so as to satisfy admissibility requirements? Will sufficient context be preserved so that the electronic records are usable?

- Compliance With Other Laws **B** Will the agency's use of electronic methods to obtain, send, disclose, and store information comply with applicable laws such as those governing privacy, confidentiality, recordkeeping, and accessibility to persons with disabilities? Myriad federal laws govern the use and disclosure of information gathered by the federal government. Agencies generally have developed systems for addressing such laws with regard to paper-based information. Electronic processes also will have to be designed to allow an agency to comply with such laws.

Part III of the Guide provides both general and specific steps an agency may take to reduce the potential legal risks of moving to electronic transactions. The general steps include:

1. Conduct an analysis of the nature of a transaction or process to determine the level of protection needed and the level of risk that can be tolerated;
2. Consider potential costs, quantifiable and unquantifiable, direct and indirect, in performing a cost/benefit analysis;
3. Use available sources of expertise, such as legal, programmatic, and technical experts, inside and outside your agency, including the OMB Guidance;
4. Consider developing a comprehensive plan when converting a traditional process to an electronic one, especially if converting means re-engineering the existing process;
5. Consider the kinds of information relevant to the process and ensure that necessary information is gathered;
6. Consider using a "terms and conditions" agreement;
7. Incorporate an appropriate retention and access policy for the records produced by electronic processes, including long-term retention where necessary;
8. Be aware of legal concerns that implicate effectiveness of or impose restrictions on electronic data or records;

9. Just as should be done with paper processes, document the various steps in your electronic process so that you can demonstrate the reliability of your process to courts and others who must determine the facts underlying an agency action;
10. Analyze the full range of technological options and follow commercial trends where appropriate;
11. If an agency considers using an outside entity to manage information, the agency should consider the various liability and privacy issues that may arise as a result of this system; and
12. Retain paper-based information in important or sensitive contexts where necessary.

The specific suggestions in Part III detail the types of information that should be gathered, retained, and made available on demand. They also make recommendations that address particular agency activities, including contracting, regulatory programs and other programs that require reporting of information, and benefit programs.

Appendix A provides key legal issues for agencies to consider in adopting an electronic process. The appendix is intended to serve as a resource for agencies; it is not a required checklist and it is not an exhaustive listing of the possible issues such processes may raise. Appendix B provides the names and contact information for the attorneys who may be contacted should readers have specific questions or comments about this Guide .

LEGAL CONSIDERATIONS IN DESIGNING AND IMPLEMENTING ELECTRONIC PROCESSES: A GUIDE FOR FEDERAL AGENCIES

U.S. DEPARTMENT OF JUSTICE

TABLE OF CONTENTS

November 2000

LEGAL CONSIDERATIONS IN DESIGNING AND IMPLEMENTING ELECTRONIC PROCESSES: A GUIDE FOR FEDERAL AGENCIES

U.S. DEPARTMENT OF JUSTICE

INTRODUCTION

Under the Government Paperwork Elimination Act (GPEA), Pub. L. No. 105-277, '' 1701-1710 (1998) (codified as 44 U.S.C.A. ' 3504 n. (West Supp. 1999)), Federal Executive agencies [1] are required, by October 21, 2003, to provide for (1) "the option of electronic maintenance, submission, or disclosure of information, when practicable, as a substitute for paper," and (2) "the use and acceptance of electronic signatures, when practicable." The Office of Management and Budget (OMB) has developed guidance to assist agencies in implementing GPEA's requirements. "Procedures and Guidance; Implementation of the Government Paperwork Elimination Act," 65 FR 25508, May 2, 2000 ("OMB Guidance"). As part of the OMB Guidance, the Department of Justice is charged with developing, in consultation with federal agencies and OMB, practical guidance on legal considerations related to agency use of electronic filing and recordkeeping. The purpose of this Guide is to identify legal issues that agencies are likely to face in converting to electronic processes and to provide some suggestions on how to address them. Agencies should also consider the significance of the "Electronic Records and Signatures in Global and National Commerce Act" (E-SIGN) (Pub.L. 106-229, § 1, June 30, 2000, 114 Stat. 464, codified at 15 U.S.C. '' 7001 -- 7006), although a detailed discussion of that statute's impact on the federal agencies is beyond the scope of this Guide.

The rise of electronic commerce offers agencies exciting opportunities to convert -- or redesign -- paper-based processes to electronic ones. While some agencies have experience using electronic processes, others are just beginning to examine the opportunity of electronic processing, or are just beginning to consider electronic processing for more sensitive transactions. In moving to electronic processes, agencies face many important decisions. Among those decisions is one crucial question of interest to the Department of Justice: when an agency converts each type of transaction to an electronic-based process, how should the agency design that process so as to protect its legal rights and minimize legal risks that may compromise the agency's mission?

In accordance with the OMB Guidance on GPEA, agency considerations of cost, risk, and benefit, as well as any measures taken to minimize risks, should be commensurate with the level of sensitivity of the transaction. Low-risk information processes may need only minimal safeguards, while high-risk processes may need more. In the context of legal and litigation risks, "low-risk information

---

[1] GPEA, Section 1710(2), refers to 5 U.S.C. 105, which provides: "For the purpose of this title, 'Executive agency' means an Executive department, a Government corporation, and an independent establishment."

processes" are those that have a small chance of generating significant liability, financial impact or litigation that would have a significant effect on the agency.[2]

The many potential benefits of re-designing (or designing) agency processes to use electronic-based processes are readily apparent: increased efficiency, accessibility, and reliability. Some agencies are already seeing benefits from increasing their use of and reliance on electronic recording and transaction systems. Yet, these benefits may not be fully realized unless the agency designs its processes with care. The collection and management of electronic records is becoming increasingly important for federal agencies.

Agencies must electronically receive, transmit, and store information in ways that will be acceptable to their program participants and others, while not violating legal restrictions, jeopardizing the government's legal rights, or unduly exposing the government to liabilities, criminal acts or other waste, fraud or abuse. The shift away from paper-based records raises serious record collection, management and retention issues, some of which are familiar to the world of paper records and some of which are unique to electronic record retention and retrieval. On the other hand, electronic records can offer benefits, like easier search and retrieval, that may reduce some of the problems of paper-based records management. Thus, the objective of any conversion to electronic processes is to maximize the benefits that such systems can offer, while simultaneously minimizing any risks, including legal risks.

The term "electronic processes" includes any use of computers or other electronic devices to conduct transactions or business, to store data or records, or to transmit communications or information (whether text, voice or visual images). Electronic processes encompass not only the hardware and software applications, but also the personnel, procedures, and policies that make the system work properly.

This Guide raises issues that agencies should consider in deciding when each of their processes and functions should be partially or entirely converted to an electronic process and how such electronic processes should be designed in order to reduce legal risks that may be identified. The first two parts of this Guide discuss the importance of the legal issues to the conversion process and explore the issues that electronic processes present to the agencies. The last part provides a list of suggested steps that agencies may incorporate into their decision-making process to address the issues raised in Parts I and II. The reader who already recognizes the legal issues presented by electronic processes and those involved in replacing paper processes with electronic ones may wish to turn first to Part III, which does not depend on the analysis of Parts I and II for understanding of its suggestions. [3]

---

[2] For example, even small transactions that take place in great volume could expose the agency to a large overall risk, even though each particular transaction does not.

[3] Further information on the topics discussed in this Guide may be obtained by contacting the lawyers whose names appear in Appendix B.

This Guide is intended only to provide information and analysis to the Department's client agencies. It is intended only to assist those agencies in identifying general issues in process design and is not intended to provide binding rules or standards for the use of electronic processes. The Department anticipates that agencies will exercise their own discretion in determining how to address the issues discussed in this Guide. Nothing herein is intended for use in resolving particular cases or to confer any right on any person or group. See, e.g., United States v. Caceres, 440 U.S. 741 (1979). The function of providing opinions and legal advice to executive agencies is conferred by regulation on the Office of Legal Counsel. 28 C.F.R. §0.25 (1999). To the extent that an agency seeks the legal opinion of the Department of Justice regarding these matters, we recommend that the agency contact the Office of Legal Counsel.

I. WHY AGENCIES SHOULD CONSIDER LEGAL RISKS

Government agencies are enmeshed in law: they are creatures of law; they act pursuant to legal authority; they are bound to carry out legal duties in a way legally accountable to the public; and they are subject to special restrictions imposed by law. For example, government procurement processes are regulated by law. Over time, agencies have developed processes to respond to obligations and practices imposed by these responsibilities. Therefore, agencies should be aware of the legal implications of converting or re-engineering existing processes and the legal changes that can occur in the move from traditional to electronic processes.[4]

Advances in technology, public expectations, Congress's mandate in GPEA, and Administration policy all require that agencies of the United States government move expeditiously to adopt electronic processes. As this Guide explains, it is important to consider carefully the legal requirements and risks associated with the process involved. In many cases, the legal aspects of the process may be apparent and adopting an electronic process may be comparatively simple. In others, designing an electronic process that adequately protects an agency's ability to carry out its programs and legal obligations, and that deters fraud and misconduct by private parties, may be more difficult. In such cases, adopting electronic processes may require a substantial and long-term commitment of agency staff and resources, including close involvement at an agency's highest levels.

Finally, we note that our comparisons in this Guide of electronic processes to paper systems should not in any way be taken as an endorsement of the continued use of those paper processes.

---

[4] The term "electronic process" is intended to encompass all systems in which records may be created or stored in electronic form as part of the agency's overall electronic process. These systems may or may not fall within the strict definition of an "electronic recordkeeping system," as defined by the National Archives and Records Administration. See 36 C.F.R. '' 1234.2, 1234.22 (1999). Adherence to laws governing federal records is one of the legal considerations involved when agencies convert to electronic systems.

Rather, because everyone is familiar with paper systems, we refer to those systems to assist agencies in issue-spotting as they develop their electronic processes.[5]

A. Legal Issues Involved in Conversion to Electronic Processes

Agencies keep records for several reasons: to carry out their public responsibility to conduct agency business with due care in a fiscally responsible manner, to meet statutory recordkeeping requirements, and to provide the information necessary to protect the government's interest when disputes arise over agency operations. Paper-based systems of records have evolved over time to satisfy those needs. Many of those systems are being replaced by electronic processes that are being deployed over short time periods. Often, problems arise because the re-engineered process does not fully capture the needs of the agency. As a result, the adoption of electronic systems, or the conversion of paper-based records systems to electronic ones, can present significant legal issues that need to be identified and addressed as part of the decision-making process. New legal issues may arise from the use of the new storage media and the new electronic mechanisms that allow agencies to conduct business and deal with the public in a manner that was not possible in the paper world. On the other hand, other legal issues may be reduced with an effective electronic process. For example, the use of a digital signature on a document can cryptographically bind the signature to the entire document, whereas a written signature on the last page of a such a document may leave questions as to which of the preceding pages are part of the signed document.

Electronic processes can be designed in such a way that the electronic transactions and their terms can be recorded in a legally adequate manner. For example, an agency can design its electronic processes so that program participants can readily ascertain when they become eligible for benefits and the agency can establish that program participants agreed to certain limitations on the agency's obligations. Even if it is determined that some legal obligations cannot be established electronically, perhaps most of the program's business can be conducted and recorded electronically if just a few crucial paper instruments are used and saved.

B. Identifying Legal Issues

At this point, no one can provide definitive guidelines as to what program safeguards will ultimately be necessary to protect an agency's interests and create binding and enforceable obligations on the agency and those with whom it does business. What we can say, however, is that agencies should attempt to understand which risks have increased and which have decreased through the adoption of electronic processes. If agencies incorporate within their processes mechanisms to account

---

[5] By the same token, we do not mean to imply that all existing paper systems are well designed (or indeed even capable of being designed) to eliminate such risks, or that well-designed paper systems are always properly implemented. That this Guide does not elaborate at length on problems with some paper transaction systems is due, in short, to its focus on electronic systems rather than any belief that paper systems are always adequate to satisfy agency needs or legal requirements.

for those risks, they will be far less likely to be surprised by unfavorable rulings than an agency that simply converts paper systems to electronic ones without undertaking such an analysis. The act of addressing these risks will give agency decision-makers a better understanding of the differences between paper and electronic processes and put them in a better position to design and implement electronic systems that will preserve the strengths of paper processes while avoiding the weaknesses inherent to paper and the flaws that have been incorporated into the paper systems over the years.

A key question agencies face in converting to or adopting electronic processes is whether the system under consideration meets the applicable legal requirements and provides adequate evidence of its transactions and actions. In certain situations, an agency may determine that an electronic process is "good enough" to meet its legal needs without regard to whether it is comparable to or as good as its prior process. At the other extreme, some agencies may decide that electronic conversion will require a complete re-engineering of their business processes in order to address the legal risks and issues that a particular system presents or that are not being addressed as effectively in their existing system.

Because most of our common experience and legal precedent comes from the paper-based world, many agencies will use their existing paper-based systems as a reference point in their analysis. So long as agencies recognize that most paper processes have risks associated with them, they may wish to consider whether the new systems will work at least as well as the traditional ones, and consider the significance of the risks posed by their conversion. The discussion that follows compares some aspects of paper systems to electronic processes as a method to identify legal issues that need to be considered in designing electronic processes. No disparagement of electronic processes, nor praise for paper ones, is meant by this analytical device.

Well-designed paper systems have advantages: paper records are more or less permanent; alterations usually can be detected; important contextual information may be added as the paper is processed; access to documents often can be controlled easily; many documents can be preserved for long periods of time and remain readable without special equipment; and there are well-settled rules that have developed over time to address issues such as the validity, authenticity, and reliability of paper documents. But paper also has limitations: storage of paper documents consumes vast amounts of space; single documents may easily be lost or become irretrievable; access is limited to those having physical possession of the document or a copy; extracting information from multiple paper sources is difficult and time-consuming; search capabilities are limited; some paper deteriorates and can become unreadable within a few years; and paper is bulky and difficult to transport in large volumes. By contrast, effective electronic processes can overcome some of paper's weaknesses: electronic records, when properly organized or archived, are easier to store, search, and retrieve than paper and allow for much broader access than paper documents.

An example describing both an agency's traditional process and its electronic process serves to illustrate this point. Suppose that an agency program involves transactions with an individual, and that the agency receives data about the transaction not only from the individual participant (e.g., an application form, financial statements), but also from other sources (e.g., agency personnel's reports on the transaction). In the traditional paper-based system, the agency probably would have kept a file

with the specific paper documents submitted by each source (e.g., the paper application form and financial statements from the participant, and internal reports from agency staff). If a dispute ever arose that required a determination of who submitted what information, the paper documents in the file probably would reflect the needed information. (If the system were flawed, however, misfiled paper documents might not be retrievable at all.) A well-designed electronic process should ordinarily be able to provide the same information as the paper system: who submitted the information; what information was submitted; when the information was submitted; and whether all the relevant information was retrieved.

Agencies traditionally file paper communications by subject or by a name of a person or entity. The challenge in such a system is to ensure that all communications are properly filed in the appropriate place. When such a system works properly, agency employees (and the lawyers who represent the agency) have a permanent record (typically arranged chronologically) of all the significant documents pertaining to the matter. When it does not, documents may be irretrievably lost through misfiling. Electronic documents, on the other hand, may be maintained in a way that uses identifiers to associate the documents with a particular matter or "file," which often allows for easier access. However, for certain types of electronic records systems, processes and procedures must be developed to address such issues as creating accurate and correct associations in the electronic files, ensuring that each document is maintained in an unaltered state, and identifying the source, date, and content of additional information added.[6]

C. Assessing the Significance of the Risk

An agency that routinely found itself able to enforce its programmatic requirements when they were embodied in written documents could face significant problems if it converts to an electronic process that does not capture information legally sufficient to enforce its interests. The full scope of agency operations can be affected by the government's ability to litigate successfully any disputes involving agency programs and operations. The outcome of litigation can dictate whether an agency can:

- collect money owed it on various loans, grants or other debts;
- enforce security interests it received to secure various financial transactions and thereby protect a lending or granting program;
- enforce important regulatory requirements;

---

6 As electronic mail ("e-mail") becomes a more common means of official communication and deliberation concerning agency actions, an agency's e-mail records will become a more significant repository of significant information reflecting agency deliberations, actions and decisions. Where an agency elects to preserve e-mail records electronically, the agency should design its electronic processes properly from the outset, to ensure that its e-mail system has appropriate mechanisms for capturing and storing those e-mail messages that ought to be a part of the official record.

- # continue to interpret its program, statute or regulations in accordance with current practices;
- # enforce contracts with third parties that are necessary for the successful running of its programs or mission; or
- # avoid unintended liabilities.

To be able to protect the government's interests in litigation, the Department of Justice needs available, reliable, and persuasive agency records: records that are complete, uniform, easily understood, easily accessible and have been kept under a system that ensures a chain of custody of submissions and information gathered from all sources. Those requirements will not disappear merely because the medium of transactions changes from paper to electronic.

Even relatively infrequent litigation can have a very substantial impact on an agency. A government victory in a single case may provide binding precedent that approves an agency practice or establishes the validity of agency regulations. Conversely, a loss in a single case might establish adverse precedent that rejects an agency practice or even invalidates an agency regulation. The agency may be able to seek a different result in future cases, but an initial loss may generate precedent that will affect the outcome of those cases, and may open the door to litigation by other parties who might not even have been aware that an argument was available. Even disputes and litigation over monetary claims against an agency may establish controlling interpretations of statutes and regulations. On the other hand, agencies should note that for transactions that an agency determines have low risk of being involved in litigation and that involve low financial risk, many of the considerations described in this Guide may not apply.

Moreover, while criminal prosecutions and civil fraud cases involve a relatively small number of transactions within any given agency, such actions are critical to the integrity of agency programs because they serve to deter others from engaging in similar conduct. When an agency does not have a credible deterrent to fraud through vigorous detection and prosecution policies, fraud typically increases dramatically. Without effective and successful litigation on the agency's behalf, fraud in agency programs may increase and legal challenges to agency actions could have a greater chance of success. Essential to such litigation is the consistent accuracy and reliability of an agency's recordkeeping system, whether paper or electronic.

Finally, agencies must be able to satisfy a variety of people besides judges and juries. Agencies are accountable to the public, customers, auditors, and Congress, and may have varying legal obligations to each. Electronic processes sufficient to protect an agency's position in court should also be able to address any legal responsibilities to these other audiences just as well-designed paper processes.

II. LEGAL ISSUES TO CONSIDER IN "GOING PAPERLESS"

As an agency identifies processes for conversion from paper to electronic, the agency should ask how it should design those processes so as to protect its legal rights and minimize legal risks that may compromise the agency's mission.

In answering these questions, agencies should consider the following four issues:

> (1) Will the electronically gathered and stored information be collected, retained, and accessible whenever needed?
>
> (2) Will the electronic collection, transmission, or storage of "documents" or information comply with applicable legal requirements, including, for example, laws requiring that certain records be maintained in a particular form or format?
>
> (3) Will electronic records be sufficiently reliable to be useful to Congress, agency decision-makers, private disputants, judges, juries, and others who must determine the facts underlying agency actions?
>
> (4) Will the agency's use of electronic methods to obtain, send, disclose and store information comply with applicable laws, such as those governing recordkeeping, privacy, confidentiality, and accessibility?

Our discussion of each of these issues is an attempt to assist the agencies in spotting relevant issues; this discussion is not intended to provide authoritative answers or to endorse any particular technology.

A. Availability of Information

To ensure the availability of information in an electronic process, agencies should ensure: (1) that an electronic process collects all relevant information; (2) that the information is retained properly; and (3) that the information is readily accessible. The potentially lengthy period of time between the collection of information and its use in many situations, including litigation, highlights the importance of these issues.

Most agencies now file and retain significant paper documents themselves. Some agencies converting to electronic processes have considered requiring the party that submits electronic information to retain the original form and source documents relating to the filing, perhaps in paper and perhaps electronically. Other agencies, recognizing the technical complexity of electronic records management, may hire contractors to maintain the information and provide more than ministerial support. If agencies rely on the people or entities submitting information to retain legally significant documents, they might find some of those documents unavailable if a dispute over the transaction arises. Similarly, if an agency uses an outside information manager, it should contractually ensure that its

information is properly retained and that the agency has access to its own information. In either case, the agency should take appropriate steps to ensure that information in third-party hands is available when needed.

1. Will the electronic process gather necessary information?

Agencies should carefully examine the processes that they will be converting to electronic processes, and determine what information must be collected from each transaction. In adopting electronic processes, agencies should ascertain whether the following four specific types of information should be captured and retained: (1) content of the transaction, including all records that comprise the substance of the transaction or filing; (2) records that contain information about how the transaction was processed, including dates received and changes or modifications that were made in records; (3) a means to authenticate the identity of all people who participated in the transaction both inside and outside the agency, and the scope of each person's participation; and (4) for appropriate transactions, a means for establishing the intent of the participants to enter into the transaction or agreement. See also, e.g., Public Citizen v. Carlin, 184 F.3d 900, 910 (D.C. Cir. 1999) (discussing preservation of content, structure, and context of federal records).

Information gathering issues can be demonstrated through the following example:

> *An agency operates a direct loan program. Formerly, the agency received loan applications on paper, but now receives them electronically through its web site. Four applicants (Abel, Baker, Company and Donald) submit loan applications that contain materially false and misleading information. When challenged by the agency, Abel, Baker, Company and Donald offer the following excuses:*
>
> - *Abel claims that he sent his application along with an explanatory electronic note that concerned key information on his application.*
> - *Baker claims that he submitted truthful information, and that someone must have altered it after he sent it.*
> - *Company, a large corporation, claims that no employee was authorized to apply for a loan, so a rogue employee (identity unknown) must have sent the application without the company's knowledge. The agency's electronic process does not show who or even what office at Company submitted the application.*
> - *Donald claims he was only working on a draft application with only preliminary information that he never meant to send, and that he must have pushed the "enter" button by accident, thus unwittingly transmitting his "draft" as though it were a real application.*

Does the agency's electronic process provide adequate safeguards, just as paper processes must, to refute the arguments raised by Abel, Baker, Company and Donald?

Content. When agencies collect information in paper form, additional information beyond that requested by the four corners of the form is frequently supplied. The document received by an agency might include additional attachments not necessarily required, and the agency might supplement the record with interlineations or notes. The physical composition of the document can attest to its completeness – for example, pages that were stapled together by the sender suggest that this was the document that was intended to be submitted to the agency. The agency's electronic process should include safeguards so that an agency can establish all of the information that was submitted by the sender as a single electronic document.

In the above example, the agency's electronic process should be designed in such a way that the agency can demonstrate that Abel's submission included only the application form and no attached electronic note or other information. In a paper system, the agency would point out that it has standardized its filing procedures in a way that ensures that all attachments are saved with the documents. (Of course, this presumes that the agency has such standards.) Abel would be faced with convincing the agency or a court that he did, in fact, include an attachment to his filing. In the electronic as in the physical world, the agency must also be able to show that its processes have been designed to capture entire communications and that its files contain everything that it received from Abel.

Processing. Agencies should also ensure that their electronic processing captures all relevant information, such as when and where the document was sent and received and whether the document was subsequently altered, and, if so, the source, date, and content of the alteration. Electronic systems can be designed to capture such information, including alterations or changes to a document. In the above example, if the agency's electronic process reliably kept track of all alterations to the applications after receipt, it could prove that Baker's application was not altered.

Identities. Often it is crucial to be able to prove who (i.e., a specific individual) submitted a communication or agreed to a transaction with an agency. Paper documents generally accomplish this fairly well, most commonly by containing a handwritten signature that can be matched with a specific person, a letterhead or return address on the document or envelope, and so on. Some transactions are so important that agencies require a personal appearance before some designated official in order to establish identity, e.g., having a notary endorse or certify the signature.

Agencies should consider whether, in appropriate circumstances, a proposed electronic process will gather information sufficient to identify the person who submitted a communication or agreed to a transaction. For important transactions, particularly those that require proof of an individual's identity, or that he or she is creating a legally binding obligation, an agency may wish to require those individuals to employ some form of electronic signature. In the above example, the use of a digital signature could provide the agency a reliable means of identifying the name, position, and

location of the specific individual who submitted the document, and thus, it would be difficult for Company to deny that one of its employees filed the application. See the discussion below in Section II.B.2 regarding the legal significance of signatures.

Intent of the parties. Enforcement of an agency's rights often depends upon being able to prove what was intended by a communication. Did the parties intend a transmission of information to be a draft of a possible contract or a final, legally binding contract? Did an individual who transmitted information to the agency intend it to be a formal report which, if false, could result in his criminal prosecution? Paper-based transactions and communications typically answer such questions in a number of ways, for example, by whether a document "looks" like a contract or just an informal letter, whether it contains a handwritten signature, or whether it contains a warning that it is submitted under "penalty of perjury." Similar methods can be used in the electronic world.

The agency could probably defeat Donald's argument in the above example by showing, for instance, that (1) its electronic process would not allow an application to be transmitted unless Donald had clicked "yes" after being shown a message explaining that by doing so, he was submitting a final application upon which the agency would rely; (2) it had provided a telephone number or e-mail address for Donald to notify the agency that an application had been submitted in error; or (3) the agency had actually notified Donald that it had received his application.[7]

2. Will the information be retained?

Audits, Congressional inquiries, litigation and other dispute resolution often take place years after the agency's acts and transactions occurred and the "files" are considered closed. But such information remains essential to the agency's abilities to protect its program and to the ability of the Department of Justice to investigate and litigate the agency's cases. Information no longer necessary for day-to-day operations also may be useful to the agency itself (for example, when agencies update procedures and revise regulations). Additionally, different types of information require different levels of retention. Thus, agencies should determine which information should be retained and for what period of time, as well as which information may be discarded soon after receipt.

Electronic systems should be designed and maintained to guard against data corruption, whether through accidental deletion, equipment failures, storage media deterioration over time, stray electromagnetic forces, or myriad other hardware and software problems. Such systems should also be designed to limit access to authorized users -- for example, by requiring controlled password identification for access to certain information. Finally, an electronic system should be designed to ensure proper file retention and tracing of alterations and updates (as to source, date, and content, and

---

[7] Equally important is the need for any system -- paper or electronic -- to identify and authenticate the government employees who acted on or approved the claim or transaction, and to record all pertinent information about their actions.

all other internal controls that are required to produce a secure and reliable record maintenance and retention system). [8]

Electronic data are frequently transferred or converted from one storage medium or software system to another. In this process (sometimes referred to as "data migration"), important information, such as formatting and the structure and content of electronic forms, may be lost, or even the record itself destroyed unless appropriate steps are taken. Similarly, unless such changes are thoroughly documented, it can be difficult to demonstrate that the critical information was not changed in the process. In transition between systems, agencies sometimes maintain multiple, overlapping systems, particularly in the transition from paper to electronic based systems. Because information from all systems may be required to be maintained under the Federal Records Act, [9] and may be needed for various purposes, agencies should address retention issues for all systems, even overlapping ones.

3. Will the information continue to be accessible?

Unlike paper files which, when properly organized and maintained in the ordinary course of business, are readily available and usable without any special equipment, electronic information is not always accessible without special equipment and software. Agencies should consider several factors related to the accessibility of electronic records. First, computer technology is rapidly changing and software and formatting standards may quickly become obsolete. Computer-stored data may become useless unless the agency can provide the continued capability with the older technologies or can accurately translate the document as more modern systems are implemented. Second, if in the future, an agency no longer has staff who are familiar and competent to work with the electronic processes necessary to read older data, such data could be functionally unavailable.[10] Electronic files might be stored while encrypted by software or protected by passwords no longer available or remembered years later, unless steps are taken to preserve the software or passwords. As noted above, these concerns are no less serious if the information is held by an outside party.

---

[8] Paper systems, of course, have their own retention and access control problems. Paper can be destroyed by age or by fire, or the warehouse in which it is kept can be made inaccessible. Moreover, paper records are expensive to store and can be difficult to locate. Employees must remember to secure sensitive records under lock and key to prevent unauthorized access. Federal agencies are generally familiar with these concerns. Electronic record systems properly implemented may provide many advantages over their paper counterparts.

[9] 44 U.S.C. §§ 2101-2118, 2901-2910, 3101-3107, and 3301-3324

[10] See Jeff Rothenberg, Ensuring the Longevity of Digital Documents, Scientific American, January 1995, at 42-47.

B. Legal Sufficiency of Electronic Records

Various state and federal laws require that certain types of transactions or events be reflected by written or signed documents. Case law and other legal authorities offer some guidance as to what types of transactions are covered and what types of records satisfy such requirements. GPEA addresses this situation by providing that electronic records and signatures shall not be denied legal effect because they are in electronic form. The recently enacted E-SIGN legislation contains similar provisions as to certain transactions, but a discussion of its provisions is beyond the scope of this Guide.

1. The importance of writings

In many circumstances, the law requires that the terms of an agreement or other legal obligation be in "writing." [11] The essence of the "writing" requirement is to establish a record that is not subject to imperfect memory or to competing claims as to what parties to an agreement intended. The formal requirement that legal documents be reduced to "writing" has been justified on many bases, including: providing the type of ceremony needed to make the parties appreciate the fact that they are undertaking enforceable legal obligations; creating evidence that the legal instrument exists and was entered into; simplifying litigation by narrowing the scope of relevant evidence; and providing evidence more permanent than a witness's recollection.

A statutory "writing" requirement does not necessarily imply that this writing must be on paper. Indeed, E-SIGN and GPEA may limit the courts' authority to restrict the term "writing" to paper documents. But the functional purposes underlying a "writing" requirement are important, and courts might require that these purposes be satisfied (whether through interpreting the term "writing" or in some other fashion) whether a document is on paper or is in electronic form. Electronic documents that satisfy the purposes of the "writing" requirement should be acceptable to the courts so long as they have the same (or better) indicia of reliability as their paper counterparts. Thus, electronic documents that provide a documentary recording of a transaction in a manner that establishes and memorializes the terms should constitute a "writing." To the extent that an electronic document is more like a traditional "writing" than an oral agreement, it should be treated by the law similarly to a paper document.[12] The challenge in creating electronic documents is to ensure that disparate communications (such as exchanges of e-mail) are reduced to a single document in a manner that provides evidence that the parties understand that the document memorializes the underlying terms and conditions. Electronic documents that satisfy those purposes are more likely to be given legal effect.

---

[11] The term "writing" is defined by statute as any "reproduction of visual symbols." 1 U.S.C. ' 1 (1994).

[12] Technology can blur the line between oral and written communications. For example, speech recognition technology automatically (without a human intermediary) converts oral statements (e.g., by phone) into text. Whether such a transmission is oral or written is a perplexing issue, and might depend upon the particular situation and statute involved.

Federal and state laws traditionally have required that many types of documents, particularly contracts,[13] be in writing and signed by the parties to be bound. State laws known as the "Statute of Frauds" also require many contracts be written.[14] See Restatement (Second) of Contracts ' 110 (1979). [15] Many states have introduced amendments that relate to electronic contracts, and these amendments are likely to have an impact on the "writing" and "signature" requirements contained in state statutory codes.

A federal statute, 31 U.S.C. ' 1501(a)(1)(A) (1994), provides that United States government obligations may be enforced "only when supported by documentary evidence of . . . a binding agreement between an agency and another person (including an agency) that is . . . in writing, in a way and form, and for a purpose authorized by law." As of the date of this Guide, no federal court has construed this writing requirement in the context of electronic commerce nor has a court squarely addressed the question of whether a purely electronic record, created as part of an automated system, would alone meet the Statute of Frauds. [16] However, case law and other legal authorities offer limited guidance as to whether federal and state statutes of frauds or other statutory requirements of writings will be satisfied by electronic substitutes. The Comptroller General has concluded, for example, that contracts formed using some electronic technologies may constitute valid obligations of the government

---

[13] "Contracts" are simply legally binding agreements between two or more parties. Government contracts can involve activities as diverse as government procurement, making and guaranteeing loans to students or farmers, and making payments to providers under Medicare and other government contracted-for benefit programs.

[14] Although the federal government's transactions generally are governed by federal law, in some instances, state laws supply the applicable rule.

[15] The Uniform Commercial Code (UCC) also incorporates a Statute of Frauds in several of its articles. Whether and to what extent a state Statute of Frauds or the UCC applies to federal government contracts can be a complex question that depends upon the circumstances. See United States v. Kimbell Foods, Inc., 440 U.S. 715, 728-29 (1979); United States v. Kelley, 890 F.2d 220 (10th Cir. 1989) (applying UCC ' 9-504 to contract with SBA guaranty contract). The UCC requires a "writing" -- defined as any "intentional reduction to tangible form," UCC ' 1-201(46) -- that is "signed." See UCC '' 2-201, 8-319, 9-203(1)(a). A "signature" includes "any symbol executed or adopted by a party with present intention to authenticate a writing." UCC ' 1-201(39).

[16] See generally R.J. Robertson, Jr., Electronic Commerce on the Internet and the Statute of Frauds, 49 S.C. L. Rev. 787, 808 (1998) ("[T]here is a substantial likelihood that courts may balk at finding that electronic messages satisfy the Statute of Frauds").

for purposes of 31 U.S.C. ' 1501, so long as the technology used provides the same degree of assurance and certainty as traditional "paper and ink" methods of contract formation. [17]

As to state statutes, many state statutes of frauds do not define "writing." However, courts have accepted electronic communications that result in a paper document at the end of the communications process, such as a telegram, as a "writing." See, e.g., Hillstrom v. Gosnay, 614 P.2d 466 (Mont. 1980).[18] To the extent that the electronic process clearly records the terms of agreements and is adequate to show that the parties intended to make those agreements -- that is, they serve the purposes that the law has required and relied on paper to serve -- it is more likely that they will be accepted by the courts.[19]

Many court systems will themselves soon be allowing electronic filing of formal pleadings and briefs. As courts become more familiar with electronic records through electronic filings, they

---

[17] National Institute of Standards and Technology B Use of Electronic Data Interchange Technology to Create Valid Obligations, 71 Comp. Gen. 109 (1991). Although opinions of the Comptroller General are not binding upon the executive branch, see Bowsher v. Synar, 478 U.S. 714, 727-32 (1986), or on the federal courts, they may offer helpful or persuasive authority. That opinion would not preclude a party in an action from asserting that an electronically formed contract was unenforceable. Thus, there exists a risk that courts would decline to enforce electronic federal contracts that have not been reduced to a traditional writing. That risk may be significantly reduced by procedures that ensure that electronically recorded transactions fulfill the purposes for which the law requires a "writing."

[18] Tape recordings of oral agreements have failed to meet the requirements of the Statute of Frauds. Sonders v. Roosevelt, 476 N.Y.S.2d 331, 331-32 (App. Div. 1984) (not a writing), aff'd mem., 476 N.E.2d 996 (N.Y. 1985); Swink & Co. v. Carroll McEntee & McGinley, 584 S.W. 2d 393, 399 (Ark. 1979) (not "signed"). See also Parma Tile Mosaic & Marble Co. v. Estate of Short, 663 N.E.2d 633, 635 (N.Y. 1996) (holding that sender's name at the top of a faxed page was not a "signature" for purposes of the Statute of Frauds where the sender's fax machine was programmed to imprint the name automatically).

[19] By contrast, courts sometimes refuse to find oral communications binding, and it will be important for agencies to ensure that their electronic processes are not regarded as so haphazard or informal that they are considered the equivalent of an oral communication. For example, courts have construed 31 U.S.C. ' 1501 (or its predecessor provision, 31 U.S.C. ' 200(a)(1) (1976)) to hold oral contracts unenforceable because they are not "in writing." So, too, could we expect the courts to reject electronic documents that are more conversation-like than formal. In In re Kaspar, 125 F.3d 1358, 1359 (10th Cir. 1997), the court refused to hold that one party's oral statement was a written one, even though the other party entered the information into an electronic document. Similarly, oral contracts alleged to have been entered into by the federal government have been denied enforcement on state law Statute of Frauds grounds. See, e.g., American Int'l Enters., Inc. v. FDIC, 3 F.3d 1263, 1269 (9th Cir. 1993) (applying California Statute of Frauds; citing other federal courts applying Statutes of Frauds from Minnesota, Nevada, and Tennessee).

presumably will become more likely to recognize the validity of records and agreements recorded solely in electronic form in sensibly implemented electronic recording systems. Courts, however, might be reluctant to interpret legal requirements liberally merely because of technological advances, and the risk that courts may lag in doing so cannot be discounted altogether.

2. The importance of signatures

Signatures have been given a unique place in the law partly because they reflect physical characteristics of individuals that were applied to the particular document at issue. Generally, the presence of a signature on a document is sufficient to identify the person who signed the document (although courts might require that someone identify the signature as belonging to the signor), to indicate that the person read and was familiar with the contents of the document (or at least had the opportunity to read it before she signed it), and to demonstrate that the person agreed and intended to be bound by the contents of the documents she signed.[20] These may be only assumptions, but agencies, businesses and the courts routinely rely on them.[21] Such "presumptions" provide a set of rules for associating an individual with a document and establishing his or her intent to accept or acknowledge its contents. Many of those rules are supported by centuries of case law and, in some cases, statutes that enforce them. Of course, signatures can be forged, may be illegible, or may have been placed on a document in a manner that does not satisfy the rules. In those situations, the party challenging the signature generally has the burden to rebut or overcome the presumption.

Unlike traditional signatures, electronic alternatives do not yet necessarily enjoy the long history of use and common expectations that surround traditional signatures. However, other steps have been taken -- and undoubtedly more will be taken in the future -- to support the validity of electronic signatures. For example, an increasing number of statutes and regulations impose the same presumptions of identity, intent, or familiarity with content that are typically associated with paper signatures. The proper design of legal instruments can reduce the need for such presumptions. Until

---

[20] Experience teaches that signatures are important to connect the individual to the act, and in some cases we have failed to prove our case where we have not had the defendant's signature. For example, in United States v. Larm, 824 F.2d 780 (9th Cir. 1987), an allergist was acquitted of Medicare fraud concerning claim forms he did not personally sign. In United States v. Brown, 763 F.2d 984 (8th Cir.), cert. denied, 474 U.S. 905 (1985), the conviction of a pharmacist was reversed on some counts because the government could not link him, through a signature or initials, to claims submitted to the government for brand-name drugs when generic drugs were dispensed.

[21] Thus, for example, courts normally prohibit individuals from avoiding their obligations by contending that they did not read what they signed, or that the contents were not explained, or that they did not understand them. In re Cajun Elec. Power Co., 791 F.2d 353, 359 (5th Cir. 1986); see Jones v. New York Life & Annuity Corp., 985 F.2d 503, 508 (10th Cir. 1993); Hill v. A.O. Smith Corp., 801 F.2d 217, 221 (6th Cir. 1986); O'Neel v. National Ass'n of Sec. Dealers, Inc., 667 F.2d 804, 806 (9th Cir. 1982).

such presumptions become widely accepted for electronic signatures, agencies should ensure that the electronic signature technologies they adopt identify the signers of the document and clearly express their intent and familiarity with the document.

For example, statutes that require certain agency officials to authorize or approve an agency action might not be satisfied with something less than a signature on a document. Thus, simply affixing a "/s/ [Named Official]" on an electronic document authorizing a particular agency action may not satisfy any requirement that agency actions be authorized in a signed writing by the appropriate official, any more than it would on a paper document. The official's signature on a paper authorization demonstrates that the official saw and signed the authorization; the law presumes that the official was aware of the contents and the effect of signing the document. To the extent that an agency adopts electronic processes for such approvals, it must ensure that the technology utilized provides a legally acceptable method for indicating approval of the action.

3. Electronic alternatives to traditional signatures

Electronic signatures generally fall into three broad methods of identifying an individual: something the individual knows, something the individual possesses, and something about the individual. Examples of techniques that use these methods include user identification codes and passwords (i.e., numbers or codes known to the individuals such as a "PIN," a passcode, or a private key used to make a digital signature [22]), tokens, smart cards or other physical objects that the user possesses that may be inserted into a reading device, and devices that measure physical, or "biometric,"[23] characteristics of the individual.[24] The National Institute of Standards and Technology has recognized that use of a

---

[22] A "digital signature" is generated by using an algorithm that ensures the identity of the signatory and the integrity of the data can be verified. Signature generation makes use of a value (commonly referred to as the "private key") to generate a digital signature. Signature verification makes use of another value (commonly referred to as the "public key") which corresponds to, but is not the same as, the private key. Each user possesses a private and public key pair, and the private key is not deducible from the public key. Public keys are permitted to be known widely, and assumed to be known to the public in general. Private keys should not be shared. Anyone can verify the "digital signature" of a user by employing that user's public key. However, signature generation can only be performed by the possessor of the user's private key. See National Inst. of Standards & Tech., Federal Information Processing Standards Publication 186-1, Digital Signature Standard, at 1 (1998).

[23] By "biometric," we mean attributes arising from a person's physical characteristics or actions that are unique to that person. These include codes derived from electronic analysis of fingerprints and retinal scans, among others.

[24] Exclusive reliance upon one biometric identification without providing any alternatives, however, may run afoul of the Rehabilitation Act, 29 U.S.C. ' 794d (West Supp. 1999), which may require agencies to provide alternative means of identification for those who do not possess the requisite physical characteristics (e.g., persons with prosthetic hands cannot provide fingerprints).

combination of authentication techniques can "substantially increase" the security of an authentication system. For example, public key digital signature technology is designed to work only when the private key which is used to make a signature is used in conjunction with the proper PIN, password, or biometric identifier. [25]

Properly implemented, various types of electronic signatures, like traditional signatures, can offer increasing degrees of reliability, although no system -- either electronic or traditional -- can completely prevent fraud or misuse. Depending on the nature of the transactions, smart cards and sophisticated digital signatures that use public key cryptography can frequently offer a reasonable degree of reliability. The risk with these technologies is that any number that can be typed or any card or token that can be inserted can also be disclosed to others or stolen. Parties seeking to avoid a transaction might claim that their identifying number, card or token was given to others who then acted as imposters.[26] Of even greater reliability is a properly implemented biometric-based digital signature. When coupled with public key cryptography, biometric-based digital signatures become an even more powerful tool that holds much promise. However, the widespread use of biometrics would be expensive to implement, its commercial application is still relatively limited, and not every transaction requires this very high degree of security.[27]

Moreover, electronic signature methods vary in their ability to ensure that an electronic document to which they are bound has not been altered after signing. Some methods provide no assurance at all, but systems using "public key, private key" digital signatures generally are designed to reveal such alterations. Thus, the better approach is to vary the level of security, depending on the significance of the underlying documents. For those records where the need for reliability is even higher, agencies should consider using a combination of security methods.[28]

---

[25] National Inst. of Standards & Tech., Federal Information Processing Standards Publication 190, Guideline for the Use of Advanced Authentication Technology Alternatives, at 39-40 (1994).

[26] On the other hand, paper signatures are susceptible to forgery. Forgeries of traditional signatures can often be detected by handwriting analysis and forensic examination. Proving that someone else used an electronic signature can be more difficult because the electronic signature has no attributes that associate it with the individual unless a biometric method is used. However, it may be difficult for an individual to explain how and why someone else was able to obtain access to an electronic signature that had been assigned to her with instructions to safeguard it and keep it private.

[27] As with other technologies, signatures in a biometric signature system that was not properly implemented might be subject to challenge. If the method of recording and preserving the signature is flawed, the signatures may not be considered reliable and may not be legally adequate to establish binding obligations.

[28] For a more detailed discussion of various types of electronic signatures, and the advantages and disadvantages of each, see the OMB GPEA Guidance, "Implementation of the Government Paperwork Elimination Act," May 2, 2000, Part II, Section 7, 65 FR at 25518.

Indeed, a well-designed electronic system can make the indication of agreement more trustworthy than paper documents that are ambiguous as to intent. The creative design of the agreement formation stage of an electronic process offers agencies the possibility to develop an indication of intent that is even more meaningful than one arising from traditional paper processes. For example, when a multi-page paper document is signed only on the last page, the question is sometimes raised whether all of the pages were included in the document the signer signed. An electronic signature bound to the entire document eliminates any question as to the contents of the document signed by the signer. With high value transactions, exceeding, rather than merely meeting, the reliability standards of paper signatures, should be an agency's goal.

4. Federal and state statutes will affect agencies' use of electronic processes

a. The Government Paperwork Elimination Act

On October 21, 1998, Congress enacted the Government Paperwork Elimination Act, Pub. L. No. 105-277, ''1701-1710 (1998) (codified as 44 U.S.C.A. ' 3504 n. (West Supp. 1999)).[29] Among other things, the GPEA provides for the development of procedures for agencies by October 21, 2003, to use and accept electronic signatures,[30] and for agencies to provide "for the option of the electronic maintenance, submission, or disclosure of information, when practicable as a substitute for paper" and "for the use and acceptance of electronic signatures, when practicable." GPEA ' 1704. Moreover, "to the extent feasible and appropriate," agencies that expect receipt by electronic means of 50,000 or more submittals are to have "multiple methods of electronic signatures" available. GPEA ' 1703(b)(1)(E).

GPEA may leave issues unresolved. For example, GPEA may not necessarily make electronic records valid and enforceable under all circumstances (any more than paper signatures are valid under all circumstances). GPEA Section 1707 provides that certain electronic records or signatures "shall not be denied legal effect, validity, or enforceability because such records are in electronic form." (Section 101 of E-SIGN contains similar language about the validity of electronically recorded commercial transactions.) While that wording bars courts from invalidating electronic records and signatures merely because they are in electronic form, it does not require courts to accept electronic records and signatures that are deficient in other respects merely because they are in electronic form. For example, if there are reasons to doubt that it was actually the electronic signature holder who affixed the signature in question, a court might not accept the electronic signature, just as it might decline to accept a paper signature that could not be verified. Also, GPEA may apply only to certain types of electronic

---

[29] Other federal bills have been introduced in Congress that may affect agencies' use of electronic processes. Agencies should monitor the enactment of any such bill into law.

[30] GPEA' 1703(a) requires the Director of the Office of Management and Budget (OMB), in consultation with others, to develop procedures for the use and acceptance of electronic signatures by Executive agencies.

signatures and to records that meet certain requirements, such as the records submitted, used, or maintained in accord with the OMB Guidance required by GPEA. [31]

b. State Statutes

Some states have enacted statutes designed to make certain electronic submissions as enforceable as signed paper documents. [32] Because those statutes might only give effect to electronic submissions that meet specified requirements, each statute must be examined for other provisions affecting the proof of the transaction, such as who (the sender or receiver) has the burden of proving whether the sender named in the transmission really sent it and whether its contents were altered. [33] Some states have enacted broader statutes, including variants on the Uniform Electronic Transactions Act (1999), which was promulgated by the National Conference of Commissioners on Uniform State Laws. It is unclear to what extent the GPEA (discussed above in Section II.B.4.a) might preempt certain of such state laws or parts of them, or the extent to which such state laws are applicable to transactions to which the government is a party or acquires an interest (e.g., government-insured loans).

C. Reliability of Electronic Information

To be useful, agency information must be reliable and meaningful. While litigators are primarily concerned about the persuasiveness of information in a courtroom, the usability of agency information affects many aspects of agency work. Agency employees must be able to rely on the information to function effectively within the agency as well as to discuss the results of agency work with those outside the agency.

---

[31] The GPEA Section 1707 safe harbor applies only to those records submitted, used, or maintained in accord with the OMB procedures required by the GPEA. That raises the question whether Section 1707 applies if an agency did not follow the OMB-mandated procedures in implementing its electronic signatures. Also, the GPEA defines "electronic signature" as: "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 ' 1710(1). A court might decline to give effect to electronic signatures that do not technically meet this definition (e.g., those that do not identify a specific person or that do not indicate that person's approval).

[32] For example, Illinois has enacted the Electronic Commerce Security Act, 5 Ill. Comp. Stat. 175/10-120(b) (West 1999), effective July 1, 1999, which provides that, subject to certain exceptions, "[w]here a rule of law requires information to be 'written' or 'in writing' . . . an electronic record satisfies that rule of law." Id. at 5-115(a). The statute does not apply to specified documents such as wills, trusts, negotiable instruments, and instruments of title.

[33] The Illinois statute (see preceding note), for example, provides that, if the parties use certain types of security procedures, then it "shall be rebuttably presumed that the electronic record has not been altered." Id. at 10-120(a).

1. The legal significance of context surrounding the collection or creation of electronic information

Any information collection system should provide a means to define, limit and show the context of the information supplied to the extent it is necessary for a particular transaction. For example, a "form" to be filled out may require specified information to be supplied on particular lines or in boxes, and such forms usually are accompanied by explanatory instructions. Completed paper forms include a means of identifying not only the answers, but also the questions and instructions. The meaning of the answers is evident from the document itself.

Electronic processes that use "forms" generally display a template of the form to the person filling it out. The person enters the information requested by the form. If the system is designed to retain and reproduce only the *answers*, and not the questions or instructions, disputes may arise over the meaning of the information supplied. Knowing an answer without knowing the corresponding question is of little value. Electronic submission systems generally should be designed to provide a copy of the form (including all questions and instructions) in response to which information was supplied to the agency, or bind the form to the answers provided. If an agency's forms change over time, and the information on the form is important either to the underlying transaction or to an agency process or program, then the electronic process should be designed to keep track of the exact form used by each submitter of information.

2. The perceived reliability of electronic data

Even though many people routinely rely on electronic information, such as electronic mail, some people are skeptical about the reliability of electronic data that are created by unfamiliar government processes. Electronic information may not be perceived as reliable if the underlying processes that create or maintain the data themselves are not viewed as reliable. For example, many people believe that information in electronic storage is vulnerable to tampering, either by internal (i.e., within the agency) or external sources. [34] The internal vulnerability concerns can be addressed by demonstrating that there are sufficient electronic procedures in place to prevent accidental or unauthorized alteration of information and to provide an audit trail to trace all changes. The concerns about external vulnerability may be met by showing that the computer system has measures in place to prevent and detect intrusions from outside and to store important information securely, off the network, where outsiders cannot obtain access to it.

---

[34] Many may have the perception that electronic data are easily fabricated or forged. People recognize that digital data can be copied perfectly, and then edited without difficulty. (Thanks to popular computer photo-processing programs, there is even a growing awareness that digital photographs can be created or modified with much greater ease than traditional photographs.) Agency security procedures that prevent such modification should be robust and well documented.

3. Persuasiveness of electronic processes and information derived from them

Because electronic processes in many respects are more complex than paper methods, explaining them or their reliability may be more difficult. Whatever systems or methods are ultimately chosen by the agency, the agency will need to provide reliable information regarding its systems (verified by periodic audits) to a variety of audiences including judges and juries, agency employees, and members of the general public with whom the agency has dealings. The agency should be able to communicate this information in a straightforward and sensible manner and should recognize that people are likely to have varying degrees of knowledge about such processes.

4. Admissibility of information derived from electronic processes

As with evidence in any form, electronic records must meet the legal requirements for "admissibility" before the government can use them in court. Generally, the party seeking to introduce records must show that the evidence is "authentic" (that is, provides proof that it is what it purports to be), and that it is the "best evidence" (that is, that it is the original or an acceptable duplicate). In addition, in order to be able to use electronic or any other agency records as evidence, the government in most cases must establish that the records were generated and maintained by a "trustworthy" process. If an electronic process does not reliably show who transmitted a piece of information to the agency, when it was transmitted, and that it has not been altered either intentionally or inadvertently, then, depending on the circumstances, the electronic record might not even be admissible, which means that the record could not even be considered by the judge or jury in deciding the merits of the government's claims or defenses. [35]

It is consequently of paramount importance that agencies using electronic processes ensure that their processes store and reproduce records in a manner that will result in records that will be admissible in court. In general, an agency's electronic processes must be able to produce reliably the information that we discuss in Section III.C., below, and any other relevant information. To determine what other information might be relevant for this purpose, agencies should consult the Department of Justice or agency attorneys who litigate the particular agency's cases.

---

[35] For example, Rule 803(6) of the Federal Rules of Evidence (FRE), generally allows records of regularly conducted activity (commonly called "business records") to be admitted into evidence. The government frequently relies upon that rule to introduce agency records into evidence. But the rule also provides that such record will not be admissible if "the source of information or the method or circumstances of preparation indicate lack of trustworthiness." Similar provisions are contained in, for example, FRE 803(8) (pertaining to admissibility of public records and reports) and 804(b)(3) (statements against interest).

D. Legal Requirements Affecting Electronic Processes

The government has long-established systems for handling paper records in ways that generally meet legal requirements regarding the use, storage, and disclosure of information. As agencies convert to electronic processes, they must ensure that those processes also facilitate and comply with such legal requirements. If disregarded, these restrictions could be a source of legal liability.

Legal requirements can affect the use of electronic processes in many contexts, some requiring that the government be able to produce or disclose information, others prohibiting the government from releasing specified information. Such requirements include:

- The Freedom of Information Act (FOIA), 5 U.S.C. ' 552 (Supp. IV 1998), requires release of certain information in agency records to members of the public upon request. This statute has been applied to computer records. See, e.g., Cleary, Gottlieb, Steen & Hamilton v. Department of Health & Human Servs., 844 F. Supp. 770 (D.D.C. 1993). The FOIA statute was recently amended to clarify the status of electronic records under public access law. See Pub. L. No. 104-231, 110 Stat. 3048, '' 1-12 (1996) (codified as amended in scattered sections of 5 U.S.C. ' 552). See also David MacDonald, Note, The Electronic Freedom of Information Act Amendments: A Minor Upgrade to Public Access Law, 23 Rutgers Computer & Tech. L.J. 357 (1997).

- Discovery in litigation. The federal government could be subject to discovery in any litigated case (even if it is not a party). [36] Such discovery can reach electronic records as well as paper records. Depending upon the circumstances, the agency might be required to gather all electronic records pertaining to a specified person, topic, transaction or event.

- The Federal Records Act (FRA) requires federal agencies to ensure adequate and proper documentation of their policies, decisions, procedures, and essential transactions, by maintaining "records" as defined under the FRA. See 44 U.S.C. '' 3101 and 3301 (1994). The National Archives and Records Administration has promulgated standards for the creation, use, preservation, and disposition of electronic records, which also specifically address the minimum requirements for electronic recordkeeping systems that maintain the official file copy of text documents on electronic media, including e-mail systems. 36 C.F.R. '' 1234.22, 1234.24(b) (1999). The government's compliance with its FRA obligations as they affect the preservation of e-mail

---

[36] See Jay E. Grenig, Electronic Discovery: Making Your Opponent's Computer a Vital Part of Your Legal Team, 21 Am. J. Trial Advoc. 293 (1997).

and word processing documents has been the subject of extensive litigation in the D.C. Circuit. See Public Citizen v. Carlin, 184 F.3d 900 (D.C. Cir. 1999); Armstrong v. Executive Office of the President, 1 F.3d 1274 (D.C. Cir. 1993).[37]

- The Privacy Act, 5 U.S.C. ' 552a (Supp. IV 1998), imposes certain restrictions on agency use of personal data. In enacting the Privacy Act, Congress was concerned predominantly with the increasing use of computers and sophisticated information systems and the potential abuse of such technology. Thomas v. United States Dept of Energy, 719 F.2d 342 (10th Cir. 1983). The Privacy Act also (1) requires agencies to provide notice about how information in a system of records is stored, accessed and used; (2) requires agencies to provide a means for subjects to challenge, correct or rebut information relating to those records; and (3) provides specific standards for computer matching of electronic records containing personal information.

- The Rehabilitation Act of 1973, 29 U.S.C. ' 701 et seq., prohibits federal agencies from discriminating against otherwise qualified persons with disabilities. Sections 501 and 504 of the Act prohibit disability-based discrimination against qualified individuals (employees and members of the public) participating in federal programs. New Section 508 of the Act, 29 U.S.C.A. 794d (West Supp. 1999), as amended in 1998, requires that all electronic and information technology systems and products used by any federal agency be accessible to persons with disabilities, including both employees and members of the public. Agencies will have to adhere to specific standards for accessibility of electronic products and systems. Section 508 also authorizes individuals to file administrative complaints or to sue agencies that have procured inaccessible electronic systems in violation of the law. [38]

- Other laws restricting agency disclosure of information, such as the Trade Secrets Act, 18 U.S.C. ' 1905 (Supp. II 1996), prohibit federal officials from

---

[37] See also Electronic Records Work Group <http://www.nara.gov/records/grs/20/index.html> (viewed Oct. 30, 2000) (collecting currently applicable guidance provided by the National Archives and Records Administration governing federal agency submission of records schedules covering the retention of electronic versions of e-mail and word processing documents).

[38] For further information about agency obligations and liabilities under Section 508, visit the Department of Justice's Section 508 home page. Section 508 Home Page (viewed Jan. 20, 2000) <http://www.usdoj.gov/crt/508/508home.html>. The General Services Administration also maintains an inter-agency web site that contains current information about Section 5008 at <http://www.section508.gov>

disclosing trade secrets or certain other types of confidential information about persons or businesses, unless authorized by law.

! Other laws and regulations require systems of records to be capable of verifying that information in an agency's possession is used solely for authorized purposes and restrict access to information for certain defined purposes and by only those agency officials who are involved in those authorized purposes. These statutes and regulations will require electronic processes to guard against unauthorized use of such information and track access to that information. (For example, 26 U.S.C. ' 6103 (Supp. III 1997) limits access to a taxpayer's tax return information to only those Internal Revenue Service employees who are directly involved in a matter involving that taxpayer; 8 U.S.C. ' 1255a(c)(2)(B)(4), (5) (1994), prohibits Immigration and Naturalization Service employees from using applications for legalization for any immigration-related purpose other than the legalization program.)

Other statutes or regulations unique to a given agency might impose further requirements or restrictions on the availability or disclosure of agency information. For example, an agency decision to allow electronic submissions by the public raises many potential issues that should be considered, such as the notice requirements of the Privacy Act, the requirements of the Rehabilitation Act, and the requirements that the FOIA may impose on access to information regarding submissions, including providing the electronic forms or templates used to capture the submission.

III. REDUCING THE LEGAL RISKS IN "GOING PAPERLESS"

The concerns highlighted in Part II, some of which have not yet been clearly decided by the courts, should not unduly deter agencies from taking advantage of electronic processes for many of their functions. Agencies should first analyze whether total conversion would be appropriate for each existing process, and examine what new processes may be needed. For those processes that are to be converted, agencies should take steps to reduce the legal risks in "going paperless."

This part of the Guide provides suggested steps that agencies may incorporate into their decision-making process to address the issues raised above. The first section of this part provides an analytic process of general considerations, and the second provides specific suggestions, including the types of information that should be gathered, retained, and made available on demand. The second section also makes recommendations that address particular agency activities, including contracting, regulatory programs, and other programs that require reporting of information, and benefit programs. These suggested steps will be helpful to agencies as they attempt to reduce legal risk when converting their processes. In accordance with the OMB Guidance on GPEA, agency considerations of cost, risk, and benefit, as well as any measures taken to minimize risks, should be commensurate with the level of sensitivity of the transaction. Low-risk information processes may need only minimal safeguards, while high-risk processes may need more. In the context of legal and litigation risks, "low-

risk information processes" are those that have a small chance of generating significant liability, financial impact or litigation that would have a significant effect on the agency.[39]

In addition, Appendix A provides key legal issues for agencies to consider in adopting an electronic process. The appendix is intended as a helpful resource for agencies; it is not intended to be a required checklist or an exhaustive listing of the possible issues such processes may raise.

A. Should Every Agency Function Be Completely "Paperless"?

Before attempting to make every agency process paperless, agencies should analyze whether total conversion would be appropriate for each process. Even if parts of an agency function are converted to an electronic process, agencies should consider whether some paper documents still should be used. The GPEA requires that, by October 21, 2003, agencies provide for "the option of the electronic maintenance, submission, or disclosure of information, when practicable as a substitute for paper," and for "the use and acceptance of electronic signatures, when practicable." GPEA ' 1704. If an agency concludes that such use for a particular type of transaction or process is not practicable, the agency is not required by the GPEA to so use electronic processes.

We note, however, that conversion to electronic processes need not be an "all or nothing proposition." An agency may conclude that it is appropriate to convert most of its processes, while continuing to use paper (at least for the time being) for one particular part of its process. This reflects the common-sense recognition that, for some important transactions, retaining a paper document might be the best, most certain, and easiest to prove medium for establishing a legally significant transaction or event.

B. General Guidelines

In considering whether each agency function or type of transaction should be converted to an electronic process, and, if so, how that process should be designed, agencies can take the following steps to address the concerns discussed above.

1. Conduct an analysis of the nature of a transaction or process to determine the level of protection needed and the level of risk that can be tolerated

Different agency functions and types of data pose different levels of legal risk. The greater the risk, the more carefully the agency should consider whether that particular function or type of data should be converted to an electronic process, and if so, how the electronic process will be designed. Riskier functions and processes dealing with more important data may require more stringent

---

[39] For example, even small transactions that take place in great volume could expose the agency to a large overall risk, even though each particular transaction does not.

safeguards when converted to electronic processes. The following types of functions are likely to pose greater legal risks:

- Transactions that have legal significance. This includes transferring funds, forming a contract or other obligation, or fulfilling a legal responsibility, such as submitting a required filing.

- Transactions open to the public. Other things being equal, transactions with the general public generally pose more of a litigation risk than transactions among agency employees or other federal agencies.

- Transactions with newcomers. Some processes occur in the context of a long-term relationship, such as a contractual or an ongoing regulatory relationship. Other transactions, such as a one-time submission of information, take place in the absence of a relationship between the submitter and the government agency, and might be riskier.

- Processes historically susceptible to fraud or litigation. These include claims for funds or reporting debts and liabilities to the government. (On the other hand, some kinds of fraud are difficult to find in a paper process, simply because human beings cannot wade through all the submissions to catch inconsistencies or patterns that warrant further investigation the way a well-instructed computer can.)

In addition, the following types of agency information or data generally need the greatest protection:

- Instruments reflecting rights and obligations. These include contracts, task orders, and other instruments by which the government or those dealing with the government undertake an obligation.

- Information traditionally used in agency litigation. For example, documents in administrative records of agency decisions or agency rulemaking, and information from agency files about individuals who are involved in disputes are often of critical importance in litigation. These and other types of information that are more likely to be needed in litigation need greater protection than, for example, generalized information on the agency's web site. Agencies might wish to confer on this point with this Department's litigating divisions that represent them in court.

- Legally protected or sensitive data. This includes data protected by the Privacy Act or the Trade Secrets Act, or information that is otherwise sensitive, such as

national security or law enforcement information, attorney-client or other privileged information, and personnel or medical records.

The above-mentioned principles should also be used to determine the type of authentication procedure needed for the transaction. Higher risk transactions should use more reliable forms of authentication, while lower risk transactions may use less rigorous methods. Such an appraisal may allow for greater security for very important transactions, while reducing the burden on agencies in connection with transactions that may not need the assurances of more rigorous forms of authentication.

2. Consider potential costs and benefits, quantifiable and unquantifiable, direct and indirect, in performing a cost/benefit analysis

Costs and benefits for government processes are not measured in strictly monetary terms. Consider whether conversion to an electronic process might change the effectiveness of the system, the amount of fraud, the amount of litigation, and the success rate in litigated cases -- all of which could impose costs or benefits on the agency. Consider the costs of complying with the legal requirements described in Section II.D, above, the cost of retaining and ensuring accessibility of data, the cost of personnel to manage the system, and other indirect costs. Consider, too, the benefits such a conversion could create, such as an increased ability to analyze data, greater ease in retrieving information, and more efficient storage of information. These various benefits and costs should also be compared to those in an agency's existing system.

3. Use available sources of expertise inside and outside your agency, including the OMB procedures

Many of the issues discussed in this Guide are unquestionably complex and draw on many kinds of knowledge, including both technical and legal experience. On legal and risk analysis issues, expertise in an agency can reside both in the General Counsel's office and in the Inspector General's office. Outside of an agency, such expertise exists in the Department of Justice. An agency might wish to consult with the particular Department of Justice components that typically litigate its cases.

As discussed above, the GPEA requires the OMB to issue procedures for use and acceptance of electronic signatures. See above at footnote 27. This guidance may be helpful to agencies. Moreover, opposing litigants might argue that the GPEA confers benefits only on systems adopted and used in accord with the OMB Guidance. Therefore, to avoid such challenges, agencies should conform their procedures to the OMB Guidance and affirmatively note their usage of the OMB Guidance on the record.

4. Consider developing a comprehensive plan when converting a traditional process to an electronic one, especially if converting means re-engineering the existing process

Agencies should design electronic processes to ensure that the processes are at least as reliable, and serve the same purposes, as the paper-based systems they replace. Agencies also should consider any existing deficiencies in their paper processes and remedy those when converting to electronic processes; they should be especially careful to identify and correct any deficiencies that will be magnified by the transition to the new system. Use of electronic processing provides unprecedented opportunities for adopting processes that would be impractical, unknown, and unimaginable in a paper-based system.

Agencies should consider developing a comprehensive plan that identifies issues and fixes responsibility for addressing those issues, including the legal concerns outlined here. In developing such a plan, an agency should encourage participation by all those affected by the conversion inside the agency, including program managers, lawyers, technical staff, persons familiar with each of the statutes that impose particular requirements (e.g., the Privacy Act, FOIA, and the Rehabilitation Act), and those interested parties from outside the agency, such as OMB and other client or sister agencies. By following such an approach, an agency is more likely to assure that all needs are being addressed during system development and over the long run, at least to the extent expressed in the plan.

For example, agencies may risk legal liabilities if their electronic processes are not designed to comply with the Rehabilitation Act, 29 U.S.C. ' 794d (West Supp. 1999), that generally requires all processes to be accessible to persons with disabilities. The Rehabilitation Act and other applicable statutes may be overlooked in the planning process unless those within the agency responsible for complying with or administering such statutes are consulted and involved in the planning process. If these issues are not addressed in the system design, agencies may risk legal liability and incur large costs in redesigning non-compliant components.

5. Consider the kinds of information relevant to the process; ensure that necessary information is gathered

Electronic processes should be designed to gather all relevant information pertaining to each transaction, including the four types of information discussed above: content, processing, identities, and intent of the parties. See above at Section II.A.1; see also, e.g., Public Citizen v. Carlin, 184 F.3d 900, 910 (D.C. Cir. 1999) (discussing preservation of content, structure, and context of federal records). In deciding what information should be gathered by an electronic process, it is useful to consider what information the agency gathers in its paper transactions or recordkeeping. To the extent such information is or might be useful or important, the electronic process must be designed to capture the same or comparable information. For example, when converting a process by which a contractor submits invoices from subcontractors supporting progress payment requests to document costs, agencies should consider ways to capture equivalent information about the authenticity of the invoices. Conversion to an electronic system also presents a useful opportunity to do a zero-assumption review

of what different or additional information, not previously gathered by paper, can and ought to be gathered by a new electronic system (and, perhaps, what information can be omitted). In some respects, a good design of an electronic system should not merely strive to replicate the paper system it replaces, but should aim at fulfilling the necessary information functions even better. [40]

6. Consider using a "terms and conditions" agreement

Agency managers could consider formalizing an agreement, sometimes referred to as a "terms and conditions agreement," among the parties to the electronic process, to ensure that all conditions of submission and receipt of data electronically are mutually known and understood. This process can assist in avoiding repudiation, rebutting a claim of ignorance, and even, where appropriate, shifting allocation of risk. Agencies should consult with their general counsel for guidance on the most appropriate terms for such agreements.

7. Incorporate a long-term retention and access policy for electronic processes

Aside from any requirements mandated by statutes or regulations governing government recordkeeping (see Section II.D, above), agencies should maintain the data that will be needed to protect their rights in litigation and otherwise. Litigation about an agency's program can take place many years after the program has come to an end, and the information to support that litigation should remain available and unaltered. The amount of time for which records must be kept varies by agency and type of data. Agencies should consult with their general counsel, the Department of Justice, or the National Archives and Records Administration for advice on these matters.

Keeping data available in electronic form means not only having the data stored on an electronic medium that is available and can be accessed through appropriate software, but it also includes having available staff or contractors who are familiar with operating the computer programs that can read data of a particular format. Auditing legacy systems can also be helpful. Further, the agency should retain the means to recover data that might have been encrypted or password-protected with long-forgotten or canceled passwords. Where agencies have multiple overlapping systems that are used during transition periods, agencies should generally retain necessary information from all of the systems.

---

[40] At the same time, an agency might wish to consider establishing a system to cull from its files genuinely extraneous and redundant information in order to prevent unnecessary bloat in agency files. Unneeded duplicates of documents and e-mail messages that the agency is not obligated to retain under its record management systems can be difficult to manage and make retrieval of relevant documents more difficult. A sensible record retention and destruction policy should provide for routine purging of unnecessary information in an orderly and regular manner. A sensible policy can also ensure that information which may be useful for ongoing contract administration or possible dispute resolution is not inadvertently deleted.

8. Be aware of legal concerns that implicate effectiveness of or impose restrictions on electronic data or records

Before permitting the electronic submission of information, agencies should review the wording of all applicable statutes and any implementing regulations to verify that electronic reporting or submission would be permitted without a legislative or rule change. The criteria agencies require for electronic transactions involving the public, such as electronic reporting, should be published to the regulated community, either by way of formal rule-making, legislative amendment, or some other appropriate means.

In addition, many uses of data are subject to restrictions under general regimes of federal law. Some agencies are subject to legal regimes that are specific to their particular work. Therefore, it may be necessary to create a mechanism for protecting disclosure of the contents of electronically transmitted information. See above Section II.D.

9. Develop processes that can form the basis of persuasive evidence

To be usable, electronic information must be persuasive. Electronic processes that can be shown to gather, retain, and reproduce data reliably and without alteration are likely to be more persuasive. Electronic processes should be designed to enhance these characteristics.

Generally, there are at least four factors that agencies should consider in developing persuasive electronic processes, which may offset each other but should be considered separately:

Simplicity and directness of the evidence. Simple and more direct evidence is generally far more effective than complex or complicated evidence.

Example: A videotape of an individual conducting a transaction would be more persuasive to many juries than a detailed examination of computer logs from the agency's system. Similarly, because fingerprints generally are familiar to most people as reliable identifiers, digitized fingerprints incorporated into an electronic signature might be more persuasive to many people than other electronic signature techniques.

Corroboration of the evidence. Rebuttable evidence can be made substantially stronger if it is corroborated by other evidence.

Example: If the evidence shows that a fraud was committed at a particular time reliably authenticated, and that a smart card used to commit that fraud had previously been issued to an individual, and that the individual had the same

smart card after the fraud was committed, it suggests that the individual had the card when the fraud took place. If the use of the smart card required the use of a password that had also been issued to the individual and the individual had not reported the loss of either, the evidence against that individual would be even stronger.

Quality of the technology at issue. Different technological solutions can provide different levels of quality for persuasiveness to the jury.

Quality of the management and implementation of the electronic process. Even the best technology can be inadequately implemented, managed, audited, or certified, leading to a loss of credibility.

Example: An agency receives an important communication from an outside party, sent in encrypted form, with an electronic signature. The agency "opens" the message, prints it in plain text on paper, and places it in the file, without keeping proof of how the message was received, or retains a copy of the data without the electronic signature attached. If the sender later denies sending the communication, the agency may be unable to prove who sent it or that it was not altered after receipt.

10. Analyze the full range of technological options and follow commercial trends where appropriate

Not all available technologies are necessarily suitable for an agency's needs, nor should it be assumed that all methods used by the private sector are necessarily appropriate for government use. For example, private institutions generally can select their customers, reducing the risk of fraud and abuse by choosing to do business only with those who appear trustworthy and by taking affirmative steps to control fraud. But many government programs are open to all comers, thus exposing government systems to greater risk. Agencies also might face greater obstacles than private businesses in implementing complex technology programs or quickly changing them as circumstances dictate. Government agencies should generally use proven technology. The government operates under legal restrictions, such as the Privacy Act, that may not bind the private sector.

11. Consider the unique legal risks presented by outsourcing an agency's data management and storage functions

Many agencies are considering using outside parties to help manage information stored in electronic form. Some agencies are requiring private parties with whom they deal to retain originals and source documents instead of filing them with the agency. Other agencies are contracting out information management and storage functions to varying degrees. The future will present creative uses of third

parties to serve many other roles, such as, for example, providing so-called "electronic notary" services to validate data and time-stamp electronic information. These creative strategies can address some agency information management needs, such as ensuring the accessibility or the reliability of information.

However, these uses of outside parties to perform data storage functions traditionally performed by agency personnel can also create a variety of additional legal risks that should be carefully considered before turning over an agency's files to a private party. In addition to other terms, contractual arrangements to provide data maintenance or storage services should, at a minimum, contain provisions providing the agency complete access to its records, specifying that the records will be kept in accord with standards that ensure the long-term availability, integrity, and reliability of the records; that the records will be legally adequate to defend the agency's rights in court or administrative dispute resolution procedures; and that the contractor's personnel will be available when necessary to authenticate records or testify as to the recordkeeping procedures.

Steps to consider include: choosing outside parties with care, clearly outlining responsibilities before initiating the relationship, placing reliance on an outside party only gradually, closely monitoring the outside party, regularly revisiting the nature and success of the relationship, taking advantage of appropriate industry standards, and developing backup plans. Agencies should especially consider the regular use and re-use of auditing or certification procedures to examine whether the outside party is following appropriate practices. Other steps may be helpful as well in reducing particular risks associated with the use of outside parties. [41]

Moreover, the use of outside parties generally will not relieve an agency of its responsibilities, such as those described in Section II.D. Any contractual arrangement should contain terms that require that the contractor meet the standards imposed by, for example, the Privacy Act, the Rehabilitation Act, and the Federal Records Act. In fact, the use of these outside parties may increase the possibility that those kinds of duties will not be met, unless the outside parties are managed with special care.

Agencies should recognize the potential problems that can arise when private parties who submit information to the federal government are required to retain originals or source documents relating to transactions with an agency. Many such documents may not be available to the agency in the future. Agencies should consider the potential impact on their programs and enforcement activities if they are unable to obtain such information.

---

[41] In one recent case where at least 43,000 electronic messages were "lost", there was a misunderstanding between the agency, which believed that backups were being made both on a daily basis and a periodic system-wide basis, and the agency's contractor, which had been doing neither. A contributing factor to the loss of the messages may have been that the audit log features had been turned off to improve system performance.

12. Retain extrinsic information in important or sensitive contexts

Even if an agency decides to implement an electronic process, prudence might still counsel for retaining paper instruments for important or sensitive transactions, or at least for the core part of transactions. For example, an agency might conduct substantial phases of a process, such as negotiation, electronically, and then formalize an agreement with a signed writing. Agencies might also consider requiring written certifications or signatures for some of their claim forms, if it would provide a helpful basis for a fraud claim years later.

C. Specific Guidelines

The following are specific guidelines for designing electronic processes to accommodate the concerns addressed in this Guide regarding the protection of agency rights, particularly in litigation. These guidelines are in addition to any recordkeeping requirements imposed by statute or regulation. Sections 1 and 2 list some of the basic information and the kinds of factual information that electronic processes should be able to reliably produce, both in general and with regard to particular types of agency functions. Section 3 suggests procedures for retention and availability of information. But these are only generally applicable suggestions, not all-inclusive lists. Agencies should not assume that, if they merely do what these lists suggest, their job is complete. Moreover, in some instances, the items we suggest might not be necessary. Each agency must assess its own transactions and programs to determine what characteristics should be built into its electronic processes.

Throughout the sections that follow, we refer to processes that are adequate to “prove” certain characteristics of the transactions described. By the term "proof" we are not referring to absolute certainty beyond all doubt. We instead are referring to evidence that will be admissible in court and sufficient to demonstrate the point under applicable law. Agency personnel with questions over what information satisfies those standards should consult with their agency's general counsel or attorneys within the Department of Justice who litigate the agency's cases.

1. General information to gather, retain, and have available

Electronic processes should be designed so that at least the following information can be proved with regard to sensitive or significant communications and transactions by, with, or within an agency:

- Date and time that the communication or transaction was sent or initiated.

- Identity and location of each particular person who transmitted such items. This includes an identifier traceable to a particular individual (e.g., digital or digitized signatures, or other identifiers, depending on which is appropriate), and a means of identifying the source of the transmission (e.g., mail server identification, e-mail account

name, time-stamped Internet Protocol ("IP") address). Identity of an individual can be established to varying degrees of certainty by the individual's transmission or use of any of the following:

- Something the individual knows (e.g., a password or secret number, personal information);
- Something the individual possesses (e.g., a token or magnetic card);
- Something the individual is (i.e., a physical or biometric attribute); or
- Combinations of the above. As we noted previously (at Section II.B.3), using a combination of techniques can substantially increase the security of an authentication system (e.g., requiring the use of a password and a token, or a unique user identification and a password).

Agencies should assess which of the above methods are suitable for each type of transaction or function, and should implement such methods in a careful way (for example, making sure that the electronic process does not readily permit someone's electronic signature to be pirated and misapplied in other transactions).

The ideal electronic signature system deployed by an agency would produce electronic signatures that are (1) unique to the signer, (2) under the signer's sole control, (3) capable of being verified by a third party, and (4) linked to data in such a manner that changes to the data invalidate the signature. The degree to which these attributes are necessary depends on the risks of the particular transaction.

Each of those attributes may be used to serve different purposes in different procedures. A password or secret number may serve a different function when creating an electronic signature, than when creating a digital signature. Additionally, a biometric attribute may be used to authenticate a transaction, or it may be used as a passcode to generate a digital signature. Therefore, agencies should be aware that these attributes can be used in isolation or combination with each other, depending on the process used.

For each process, an agency should define the roles to be played by the electronic signature and adopt the electronic signature technology or technologies that best serve those purposes. If its primary function is to prove identity, other techniques or information may provide better proof in an electronic environment than a weak electronic signature. On the other hand, an electronic means that may be unconvincing at proving identity may be adequate for other functions, such as proving receipt or proving intent.

! That the communication or transmission actually was received, by whom it was received, and the date and time it was received.

! What the sender or originator of the communication or transmission intended by it, and the date and time he or she signed it. For example, certain electronic processes should be able to prove that a person who submits a report certifies to the agency that his report is true, accurate and correct at the time submitted. If the submitter of a document is shown a banner on his computer screen on which he must click "yes," the electronic process must be able to prove that the banner (including its precise text) was in fact displayed and that he clicked "yes."

! The complete contents of the communication or transaction, including any attachments or exhibits.

  # This can include the terms unique to a given transaction and "boilerplate" terms that, on paper, might have been printed on the back of a form or in a set of instructions;

  # If the communication contains answers or responses to questions on a form, include a means of proving the precise questions, instructions, or contents of the version of the form actually used; and

  # For communication with attachments, there must be a means for preserving the attachments and permanently "binding" them to the electronic communications.

! Some means of proving that the information in the transmission was not altered. This includes proving that no one (e.g., neither the submitter nor the agency) altered the information after the submitter sent it, perhaps by proving that the electronic system allows no one the ability to alter such documents. Or the

electronic process might be designed to provide an "audit trail" showing all alterations, the date and time they were made, identifying who made them, and so on.

- As appropriate, some means of showing all relevant communications and documents on a given subject or point.

- Some means of distinguishing final documents from drafts.

2. Information regarding particular types of transactions

In addition to the preceding guidelines, electronic processes generally should be designed to provide additional or more specific information with regard to particular types of interactions.

a. Contracts and related transactions

Agencies that enter into contracts (which may have follow-on invoices or progress payment requests) or otherwise seek to enforce rights in connection with liens, mortgages, insurance, or guarantees, generally should design their electronic processes so as to be able to establish at least the following:

- Date and time of the contract or other instrument, any amendments to it, and any claims for payment (including invoices or progress payment requests) submitted under it;

- Date and time that each party submitted its offer, acceptance, or claim for payment, the date and time it was received (including proof that it was in fact received), and proof of the identity and location of each particular person who transmitted such items. This includes an identifier traceable to a particular individual (see Section III.C.1, above), and a means of identifying the source of the transmission (e.g., mail server identification, e-mail account names);

- Every term, provision and certification that applies to the transaction. Such terms include standard or "boilerplate" terms, as well as the terms unique to the particular transaction. Because agencies might change the standard terms used in later contracts, the system must be able to show what terms were in effect in each particular transaction. If the contract involves filling out a form or responding to a prior communication, then include the questions on the form or the content of the prior communication;

- That the text of all terms (specific terms and any boilerplate terms) was actually made available to each party;

- That all required parties agreed to the contract or transaction. This includes at least three components:

  - The identity of the specific individuals (see Section III.C.1, above) who entered into the contract or transaction on behalf of each party, and any appropriate identifying information about them (such as their titles, divisions, and so on);

  - Proof that the transaction was an agreement (i.e., text stating that the party or parties "agree"); and

  - Proof that each party intended to be legally bound (again, through use of, for example, an electronic signature traceable to a particular individual with authority to contract on behalf of the party, combined with proof that the "signature" was applied to that specific contract, and the date and time on which that occurred).

- Where applicable, proof that the individual has certified to the truth and accuracy of the information submitted on any claims or required certifications and has submitted the information under penalty of perjury;

- All amendments, if any, to the transaction, including each of the above items for each amendment, along with proof that no other changes, amendments, or alterations have been made by the submitter, the government, or anyone else.

b. Regulatory programs (and any programs that require reporting of information)

Agencies that accept in electronic form information that is required to be collected under statutory or regulatory programs (or in connection with contracting), and that rely on such information in the conduct of agency business, generally should design their electronic processes so as to be able to establish at least the following:

- Date and time of transmission (either date and time of transmission or date and time of receipt or both, depending on program or agency requirements) and proof that the communication was actually received by the agency;

- The identity and location of each particular person who transmitted the report or data. This includes an identifier traceable to a particular individual (see Section III.C.1, above), and a means of identifying the source of the transmission (e.g., mail server identification, e-mail account names);

- Proof that the submitting individual was authorized to report for the company or other entity (e.g., his position or title);

- Complete contents of the communication, including any attachments or exhibits. Complete contents include both data and information submitted by the individual or company and the agency forms, questions or certifications to which the information responded;

- All amendments, if any, to the report, including each of the above items for each amendment, along with proof that no other changes, amendments, or alterations have been made by the submitter, the government, or anyone else;

- Where applicable, proof that the individual has certified to the truth and accuracy of the information submitted and has submitted the information under penalty of perjury. This might include, for example, proof that a banner was displayed to the submitter, informing him that by clicking "yes" he acknowledges those matters.

c. Benefit programs

Agencies that accept electronically submitted applications or communications involving the receipt of government benefits of any kind (e.g., loans, grants, or entitlements), generally should design their electronic processes so as to be able to establish at least the following:

- Date and time of receipt of the application or communication (either date and time of transmission or date and time of receipt or both, depending on program or agency requirements) and proof that the application or communication was actually received by the agency;

- Proof of the identity and location of each particular person who transmitted such items. This includes an identifier traceable to a particular individual (see Section III.C.1, above), and a means of identifying the source of the transmission (e.g., mail server identification, e-mail account names);

- Complete contents of the application or communication, including any attachments or exhibits. Complete contents including all data and information

submitted by the individual corresponding to requests for information or certifications on an application form, as well as the substance of the requests or certifications themselves;

- Where applicable, proof that the individual has certified to the truth and accuracy of the information submitted on the application and has submitted the information under penalty of perjury;

- Where applicable, some means to prove that the confidentiality of the applicant's submission or communication has not been compromised;

- All amendments, if any, to the application, including each of the above items for each amendment, along with proof that no other changes, amendments, or alterations have been made by the submitter, the government, or anyone else.

3. Retention and availability

Once an agency determines which electronically gathered information must or should be gathered, retained and available in light of the issues discussed in this Guide, the agency should establish policies to fulfill those goals. Of course, various statutes and regulations impose requirements for the retention and availability of official records in electronic recordkeeping systems.[42] But in addition to those requirements, agencies generally should ensure that their electronic records that are important in light of the issues discussed in this Guide are:

- Retrievable in a form that can be viewed or printed in a "user-friendly" form;[43]

- Indexed in a manner sufficient to be able to retrieve needed data (for example, by subject, by name of program participant, by date and time, etc., in a manner that allows compilation of all relevant documents into a usable "file");

- Retained and retrievable in an electronic recordkeeping system for the length of time required by law, agency policy, or records retention schedules;

---

[42] See, e.g., 36 C.F.R. ' 1234.2 (1999) (National Archives and Records Administration definition of "electronic recordkeeping system"); see also 36 C.F.R. ' 1234.22; 1234.24(b) (1999) (providing functional requirements for electronic recordkeeping systems, including e-mail).

[43] To the extent that an electronic transmission includes data that cannot practicably be printed in paper form (e.g., an audio file attached to an e-mail), the agency should have some means of storing and being able to retrieve the image or sound of such items.

- **!** Fully retrievable, printable, and adequately indexed even if the agency later modifies its electronic system (hardware or software), or later changes the contractor who manages the electronic process for the agency;

- **!** Accessible, even if the electronic document originally was encrypted or restricted by a password;

- **!** Capable of being promptly located, retrieved, printed, and interpreted by staff or otherwise immediately available personnel. (Where appropriate, promptly locating a record may include locating a notation that the record itself has been disposed of in accordance with an approved records schedule.)

Agencies may need to take specific measures to ensure the long-term accessibility of data in light of changes over time in technology, personnel turnover, or changes in contractors.

CONCLUSION

As agencies move forward in adopting electronic processes and making judicious use of technology, they face many decisions. This Guide has been provided to help agencies in considering the legal aspects of such decisions and to help them design their processes in a way that will reduce their legal risk and thus fully realize the benefits of electronic processing. For further information, consultation, or to provide feedback on this Guide, please contact any of the Department of Justice lawyers listed in Appendix B of this Guide.

In accordance with the OMB Guidance on GPEA, agency considerations of cost, risk, and benefit, as well as any measures taken to minimize risks, should be commensurate with the level of sensitivity of the transaction. Low-risk information processes may need only minimal safeguards, while high-risk processes may need more. In the context of legal and litigation risks, "low-risk information processes" are those that have a small chance of generating significant liability, financial impact or litigation that would have a significant effect on the agency.[44] Agencies may wish to use the following twelve suggestions as a starting point in their analysis of legal risks:

1. Conduct an analysis of the nature of a transaction or process to determine the level of protection needed and the level of risk that can be tolerated;
2. Consider potential costs, quantifiable and unquantifiable, direct and indirect, in performing a cost/benefit analysis;
3. Use available sources of expertise inside and outside your agency, including the OMB GPEA Guidance and other OMB guidance;

---

[44] For example, even small transactions that take place in great volume could expose the agency to a large overall risk, even though each particular transaction does not.

4. Consider developing a comprehensive plan when converting a traditional process to an electronic one, especially if converting means re-engineering existing process;
5. Consider the kinds of information relevant to the process; ensure that necessary information is gathered;
6. Consider using a "terms and conditions" agreement;
7. Incorporate a long-term retention and access policy for electronic processes where necessary;
8. Be aware of legal concerns that implicate effectiveness of or impose restrictions on electronic data or records;
9. Develop processes that can form the basis of persuasive evidence;
10. Analyze the full range of technological options and follow commercial trends where appropriate;
11. Consider using outside parties to manage information as well as developing methods to manage the particular risks of doing so; and
12. Retain sufficient extrinsic records in important or sensitive contexts.

In addition, Appendix A provides issues for agencies to consider in adopting an electronic process.

APPENDIX A - KEY LEGAL ISSUES TO CONSIDER IN ADOPTING AN ELECTRONIC PROCESS

This appendix is provided as a resource for agencies to identify the legal issues to consider in adopting an electronic process. There are two general ways of identifying the legal issues associated with adopting electronic processes. One convenient approach is to consider the features of an existing paper-based process, and decide how the electronic process must be designed in order to provide the same functions. In the alternative, one can turn to first principles and seek to identify legal issues without reference to any existing process. These two approaches may be complementary; concerns that might be immediately apparent when one approach is used may not be under the other approach. Accordingly, this appendix incorporates elements of both approaches.

This appendix focuses on legal issues associated with adopting an electronic process. (This analysis has many features of a requirements analysis, which agencies might already be conducting as part of their business process.) Although electronic processes can have many significant advantages over paper processes, those benefits will not be addressed in detail as they are outside the scope of this Guide. This appendix also does not comprehensively address issues associated with archiving of records; for a more detailed review of that topic, please consult the guidance prepared by the National Archives and Records Administration. Although this appendix is intended as a resource to federal agencies, some agencies may conclude that other approaches are more appropriate in addressing legal issues related to the development, use, and maintenance of those agencies' electronic processes.

A. Comparison of paper and electronic processes

1. What is the type or purpose of the process **B** is it a benefits application, a contract, a bid proposal, a legally required report, or some other type of process?

2. What does each party to the communication need in order to achieve that purpose? This may include dates, identities, intent, signatures, the sources of particular information, and the informational content of the transaction itself. Who uses the information in your agency, and for what purpose? Are there types of information that are needed only for certain narrow purposes or only infrequently, but are very important for those purposes?

3. How will the electronic process collect this information?

4. What is it about the existing process that satisfies this need? A signature may serve a range of purposes, including proving identity and intent, and deterring abuse. Likewise, mailing of paper documents to a known address both helps to complete a transaction and helps to confirm the identity of the other party to the transaction. How will the electronic process be designed to meet these needs?

5. How do you ensure that information, once obtained, continues to be available when and where you need it? How is information organized, stored, and retrieved? When is information likely to be needed again, and for what purposes? How can appropriate availability of information be assured in an electronic process?

6. What security procedures do you have, and why? Who has access to information and who does not, and why? How can equivalent or better security be obtained in an electronic process?

7. What elements of your program and process have historically been susceptible to fraud or other abuse, and why? How do you deter these activities? How will you ensure similar or greater deterrence in the electronic process? Will evidence of abuse be as available and persuasive in the new system as in the old one? Are there any features of the electronic process that are likely to facilitate fraud, abuse or disputes that did not occur before, or conversely, that are likely to discourage such acts which have occurred in the past?

8. What do you do in your existing system to comply with applicable laws and regulations, including any signature requirements, the Freedom of Information Act, the Privacy Act, the Rehabilitation Act, discovery procedures, and confidentiality laws? How will you ensure that you will continue to comply with those laws and regulations in your electronic system?

9. Have you adopted a plan to address the issues raised by moving to an electronic system, and planned to consult relevant offices and agencies (including general counsels, inspectors general, and relevant components of the Justice Department)?

B. Legal issues raised by electronic processes

1. Have applicable legal and practical requirements been considered?

   Is any information used in the process required by law or regulation to be in a particular form, paper or otherwise?
   Is the transaction required by law or regulation to be "signed?" If so, how do you plan to satisfy that requirement?
   Will your process comply with the Government Paperwork Elimination Act?
   What steps in the plan are taken to ensure confidentiality if confidentiality is required?

Will the process comply with:
The Privacy Act?
The Rehabilitation Act?
The Freedom of Information Act?
The Federal Records Act?
Other requirements applicable to the agency's programs?

2. How necessary is the information?

Is there a legal requirement to maintain the information?
Is the information of importance to national security, public health or safety, public welfare, the protection of the environment, or other important public purposes?
How many people would be affected by the unavailability of this information?
What is the importance of the information to the agency's programs?
Could the information be used to collect money from the United States? Used by the United States in collecting money? How much money is at issue in each individual transaction? In the process as a whole?
Does the information otherwise reflect rights or obligations of the United States or of other parties?
Might the information be needed for use in criminal proceedings? In other legal proceedings?
Is the information needed for proper agency management or for maintenance of agency financial records?
Is the agency confident that the information will not be needed in the future for any important purpose?
Is the information needed for any other reason?

If the foregoing analysis reveals that the information will not be necessary in the future and is not required to be retained under applicable law, there is likely to be little need to consider the risks associated with collection, use, and retention of the information discussed below. If, however, the information is likely to be of legal significance, the agency may wish to consider the following items in addressing potential risks. If the information is a "record," applicable law may nevertheless require it to be preserved in some form. Refer to guidance prepared by the National Archives and Records Administration for more detail on this topic.

3. What are the risks that private parties will seek to commit fraud or otherwise misuse the process?

How much money or other benefits are at issue in each individual transaction? Can transactions be aggregated?

Is the transaction conducted with people with whom the agency has had a long-term relationship?
Is the program one with a history of fraud?
Are there any other reasons to anticipate fraud in this process?

4. What are the risks that information will be damaged or lost?

Will the information be stored in a way that is accessible in a timely fashion if it is needed?
Will the information be retrievable in a way that is easy to understand?
What steps will be taken to control, log, and audit modifications to stored information?
How long will the agency need to keep its records?
Is it appropriate to involve outside contractors in information management tasks?
If so, does the contract and oversight process protect the interests of the agency and the public?
What plans are in place for migration of information when system technology is upgraded?
What parts of the process are unusual, distinctive, or unique to the agency? Do these steps give rise to unusual risks of harm to stored information?
Are there other risks?

5. Will the information collected be complete?

Does an identity need to be associated with a transaction? How will identity be proved?
Does intent need to be associated with a transaction? Can the agency prove that the person who transmitted the information understood its significance and appreciated that his or her transmittal was legally binding on him or her?
Does a signature need to be associated with a transaction? If so, what is the function of the signature **B** identification, intent, evidentiary use, or some other function? What is an appropriate electronic equivalent? Is a digital signature required, or will some lesser form of electronic signature suffice?
What information about the processing of the document (such as when a document was sent or from where it was received) must be retained?
Are documents ever modified upon receipt? If so, how is information (including context, identity and intent information) regarding the modifications collected, retained, and made available? How is this information segregated from information associated with the original submission?
Is there some other necessary legal element required to conclude the transaction (delivery of a deed, for example)?

What contextual information is necessary (e.g., the questions to which a set of stored answers correspond)? How will it be collected and maintained?
Is there any information that is used only infrequently, or only for one narrow purpose, but that is nevertheless critical to the success of the system?
What other information needs to be collected by virtue of the distinctive features of the transaction?

6. Will the information be otherwise usable and credible for all necessary purposes, including possible legal proceedings?

Can the agency show that the information it received accurately reflects the information that was intended to be transmitted?
Can the agency show that the information it possesses accurately reflects the information originally submitted to it? Is the original information available as well as any subsequent edits?
Is a "terms and conditions" agreement appropriate?
Is the information retained sufficient to be persuasive to a judge, jury, or other third party? Does it provide simple, straightforward and corroborated evidence of what occurred?
Has the agency addressed any other potential obstacles to the use of the information in a legal proceeding?

7. Have all relevant offices and agencies been consulted? Potentially interested offices and entities may include:

Agency program offices
Agency information technology specialists
General Counsel's office
Inspector General's office (audit and investigative personnel)
Records management personnel
FOIA, Privacy Act, and civil rights officers
Agency enforcement personnel
Other agency personnel
Office of Management and Budget
The Department of Justice
National Archives and Records Administration
Other government offices or agencies (federal, state, local and tribal) that are involved in the process, use the resulting information, or otherwise have a stake in process design
Private and non-governmental organizations, including as appropriate contractors, the regulated community, and representatives of the general public

8. Have you developed a plan to address the foregoing issues?

Does the plan assign responsibility for particular tasks or problems to specific offices or individuals?
Does the plan provide for any auditing of the process, including auditing of any outside contractor who manages information on behalf of the agency?
Does the plan provide for periodic reassessment?
Have you consulted with interested parties on the development of this plan?
Have you shared the final plan with interested parties?

APPENDIX B - CONTACT INFORMATION

DEPARTMENT OF JUSTICE
ELECTRONIC COMMERCE WORKING GROUP
CO-CHAIRS

David Goldstone (Co-chair) Computer Crime and Intellectual Property Section, Criminal Division (202) 514-1026 (202) 514-6113 fax David.Goldstone@usdoj.gov	Chris Kohn (Co-chair) Director, Corporate/Financial Litigation Section, Commercial Litigation Branch Civil Division 202-514-7450 202-514-9163 fax Chris.Kohn@usdoj.gov

DEPARTMENT OF JUSTICE
ELECTRONIC COMMERCE WORKING GROUP
ELECTRONIC PROCESSES SUBGROUP

Tony Whitledge (Chair) Criminal Appeals and Tax Enforcement Policy Section, Tax Division (202) 514-2832 (202) 305-8687 fax Tony.Whitledge@usdoj.gov	Marc Gordon Land Acquisition Section, Environment and Natural Resources Division (202) 305-0291 (202) 305-8273 fax Marc.Gordon@usdoj.gov
David Goldstone Computer Crime & Intellectual Property Section, Criminal Division (202) 514-1026 (202) 514-6113 fax David.Goldstone@usdoj.gov	David Gottesman Corporate/Financial Litigation Section, Commercial Litigation Branch Civil Division (202) 307-0183 (202) 514-9163 fax David.Gottesman@usdoj.gov

Joan Hartman Fraud Section, Commercial Litigation Branch Civil Division (202) 307-6697 (202) 616-3085/9029 fax Joan.Hartman@usdoj.gov	Jennie Plante Executive Office for United States Attorneys (202) 616-6444 (202) 616-6647 fax Jeanette.Plante@usdoj.gov
Brian Kennedy Federal Programs Branch, Civil Division (202) 514-3357 (202) 616-8470 fax Brian.Kennedy@usdoj.gov	Richard Phillips Federal Programs Branch, Civil Division (202) 514-4778 Richard.Phillips@usdoj.gov
Sylvia Liu Policy, Legislation, and Special Litigation Section, Environment and Nat. Res. Division (202) 305-0639 (202) 616-8543 fax Sylvia.Liu@usdoj.gov	Justin Smith Policy, Legislation, and Special Litigation Section, Environment and Natural Resources Division (202) 514-9369 (202) 514 4231 fax Justin.Smith@usdoj.gov
Ken S. Nakata Disability Rights Section, Civil Rights Division (202) 307-2232 (202) 307-1198 fax Ken.Nakata@usdoj.gov	