**Management Issues
in a
"Paperless" Environment**

June 1999

Inspection Report

No. 99-06-01

**Office of Inspector General
U.S. Small Business Administration**

June 30, 1999

TO: Kristine Marcy
           Chief Operating Officer

           Lawrence Barrett
           Chief Information Officer

           Michael Schattman
           General Counsel

FROM: Tim Cross
           Assistant Inspector General
             for Inspection and Evaluation

SUBJECT: Inspection of Management Issues in a "Paperless" Environment

We are pleased to submit our inspection report on ***Management Issues in a "Paperless" Environment***. The Office of Inspector General (OIG) initiated this inspection as a proactive effort to help SBA management successfully make the transition to such an environment and to identify potential security, legal, and organizational problems.

To gain the greatest benefits from the electronic exchange of information, SBA will need to allow at least limited access by outside partners to its systems. A major concern is how to balance this access with security for the systems and the sensitive information they may contain. If current trends continue, SBA will probably conduct much of its business using a Public Key Infrastructure (PKI) that employs digital signatures and identifiers called digital certificates to prove a sender's identity and a message's integrity. Implementing PKI presents challenges as well as opportunities.

To avoid excessive expenditures on protecting low-value data, the OIG recommends that the Chief Operating Officer require that each program, in consultation with the Office of the Chief Information Officer (OCIO) and the Office of General Counsel (OGC), identify the types of data requiring the highest level of security and privacy safeguards. To protect SBA's interests amid PKI uncertainties, we also recommend that OGC, in consultation with OCIO, develop contracts for use with the trusted third parties providing PKI services. The contracts would identify the parties' responsibilities, liability, and recourse.

An electronic environment raises significant concerns about privacy and the potential exposure of confidential information. To reduce such exposure, the OIG recommends that OCIO, in consultation with OGC, limit the amount of information in the digital certificates used to verify the authenticity of an electronic document. To help minimize internal security breaches, we recommend that OCIO and OGC jointly develop a notice for periodic display on computer screens to remind SBA employees and contractors of their information security responsibilities, the relevant penalties, and the fact that using Agency information systems constitutes acceptance of those responsibilities and penalties as well as consent to law enforcement searches.

A paperless environment involves a number of important legal issues, including the authentication of documents and transactions, the admissibility of digital signature evidence, and the storage of electronic information. Until uniform standards are developed, parties to electronic transactions will have to rely on contracts to spell out their legal responsibilities. The OIG recommends that OGC, in consultation with program managers and OCIO, ensure that contractual agreements with resource partners and small businesses specifically define what constitutes a valid electronic identity and signature for each party, hold each party responsible for the accuracy of the electronic information it transmits, and define each party's recourse.

Finally, based on other organizations' experiences, it would be to SBA's benefit to (1) decide which work processes should be paperless based on solid business analysis, rather than simply on the availability of advanced technology; (2) strive to make work processes and electronic systems operate seamlessly; and (3) recognize that human factors are at least as important as technology in implementing paperless solutions. The OIG recommends that a top-level official with authority over SBA programs, such as the Chief Operating Officer, lead a central coordination group of managers, staff, and technical experts to identify any major Agency work processes that could be eliminated or performed more efficiently by outside parties, identify processes that are candidates for electronic initiatives, and refer the electronic initiatives approved by the group to the Business Technology Investment Council for detailed information policy and cost evaluation.

OCIO and OGC concurred with the report's recommendations, and the Chief Operating Officer indicated her support for our findings.

The OIG inspection team appreciates the excellent cooperation received from SBA staff, other Federal officials, and representatives from non-governmental organizations. We would welcome the opportunity to brief you on this inspection at your convenience.

Attachment

TABLE OF CONTENTS

Page

ABBREVIATIONS

ABA	American Bankers Association
ACES	Access Certificates for Electronic Services
ATM	Automated Teller Machine
CA	Certification (or Certificate) Authority
DoD	Department of Defense
FOIA	Freedom of Information Act
FY	Fiscal Year
GAO	General Accounting Office
GRS	General Records Schedule
GSA	General Services Administration
IRS	Internal Revenue Service
LowDoc	Low Documentation Loan Program
MMS	Minerals Management Service
NARA	National Archives and Records Administration
NASA	National Aeronautics and Space Administration
OCIO	Office of the Chief Information Officer
OGC	Office of General Counsel
OIG	Office of Inspector General
PCIE	President's Council on Integrity and Efficiency
PCLP	Premier Certified Lender Program
PEBES	Personal Earnings and Benefit Estimate Statement
PKI	Public Key Infrastructure
SBA	Small Business Administration
SBIR	Small Business Innovation Research
SOP	Standard Operating Procedure
SSA	Social Security Administration
USC	United States Code

EXECUTIVE SUMMARY

THE PAPERLESS OFFICE

As the world's banking and financial services institutions undergo unparalleled technological changes, the U.S. Small Business Administration (SBA) and other organizations—in both the public and private sectors—are gradually moving toward "paperless" methods of conducting business. Much of this movement is spurred by the organizations' need to streamline their operations while sustaining high-quality levels of service despite reductions in staffing and other resources. For our purposes, an office is defined as having a paperless environment if its work processes are essentially electronic, with minimal use of paper documents and reduced need for human handling of routine tasks. The purpose is to eliminate the inefficiencies that a paper-based and relatively labor-intensive environment causes. Nonetheless, "going paperless" can have serious security and legal ramifications and significantly affect both an organization's work processes and its internal culture.

The Office of Inspector General (OIG) initiated this inspection as a proactive effort to identify potential problems and to help SBA management successfully make the transition to a paperless environment.

SBA's Approach to a Paperless Environment

SBA plans to become a "21st Century Leading-Edge Institution" through centralizing work processes, modernizing technology, and outsourcing portions of programs. According to Agency officials, the sizable cuts projected in staffing will compel SBA to make greater use of technology and serve more as a portfolio manager. The Agency will likely perform more oversight functions, such as monitoring preferred lenders and outsourced services, and act as a facilitator to match small businesses with resources.

If current trends continue, SBA will probably conduct much of its business through a Public Key Infrastructure (PKI), which employs digital signatures to prove a sender's identity and a message's integrity. To ensure the digital signature's uniqueness, the sender and recipient each have a public (published) key and a private (secret) key. For the keys to work, PKI requires a trusted third party—known as a certification, or certificate, authority (CA)—to vouch for the sender's identity. The CA issues a digitally signed message—called a digital certificate—binding the sender's identity to his/her public key. This certificate resembles a credit card or driver's license—an item issued by an organization having information about the user and able to verify the item's authenticity. Nonetheless, PKI raises accountability, privacy, and implementation issues.

SECURITY ISSUES

To gain the greatest benefits from the electronic exchange of information, agencies such

as SBA must take the risk of allowing at least limited access to their systems. The problem is how to balance access with security, without wasting limited financial and human resources.

According to computer security experts in both the private and public sectors, organizations attempting to secure their electronic systems should adhere to several basic principles. These include:

- Senior management needs to recognize information resources as essential organizational assets.

- The organization should identify the key information assets that require the greatest protection.

- No electronic security solution is foolproof.

- The greatest threats are internal, e.g., employees who are disgruntled or simply inattentive to security procedures.

- Because every security control has a cost, the decision to impose a new control should be based on a careful business analysis of the expected benefits.

The most important lesson from security experts is that if an organization ignores the human element, even the most sophisticated encryption, firewalls, and PKI protections may be rendered useless. Also, according to both private and public sector officials, establishing and enforcing appropriate policies and procedures are by far the most difficult aspects of enhancing computer security.

Based on the security issues discussed in this report, the OIG recommends that:

1) The Chief Operating Officer require that each program, in consultation with the Office of the Chief Information Officer (OCIO) and the Office of General Counsel (OGC), identify the types of data requiring the highest level of security and privacy safeguards.

2) The OGC, in consultation with the OCIO, develop contracts applicable to any certification authority or registration authority the Agency might use in a Public Key Infrastructure, with such contracts identifying--

- **Each certification authority's and/or registration authority's transaction and security responsibilities and liability for failure to complete an electronic transaction, and**

- **Each party's recourse if it performs a transaction based on the other's false**

or inaccurate information.

3) The OCIO, in consultation with the OGC, limit future digital certificates to the minimum information necessary to complete Agency electronic transactions.

4) The OCIO and the OGC jointly develop a concise notice for periodic display on computer screens to remind Agency employees and contractors of their basic information security responsibilities, the penalties for failure to carry out those responsibilities, and the fact that using Agency information systems constitutes acceptance of those responsibilities and penalties as well as consent to searches by law enforcement organizations.

LEGAL ISSUES

Any organization planning to establish a paperless office environment should first address a number of legal issues, including the authentication of documents and transactions, the possession of a documentable record trail, the admissibility of evidence regarding digital signatures, and the storage of electronic information.

Current Status of Relevant Laws and Regulations

The Government Paperwork Elimination Act of 1998 requires Federal agencies to recognize electronic signatures and make Federal forms available online during the five-year period beginning in 1998. The public will be able to use the Internet to access Federal forms and electronically submit them to Federal agencies.

Despite this legislation, the legal authority for disposition of certain types of electronic records is in a state of flux. In November 1998, the National Archives and Records Administration (NARA) generally endorsed a standard for electronic records management developed by the Department of Defense (DoD). This standard specifies that records management software perform the following functions:

- Assign a unique, computer-generated identifier to each record.
- Treat electronic mail messages that have been filed as records, including attachments, as any other record.
- Provide for viewing, saving, and printing lists of records (regardless of media) based on record profiles.
- Identify records that can be sent to a repository for storage.
- Notify authorized individuals when a record is eligible for destruction and destroy it after their approval.[1]

---

[1] Department of Defense, "Design Criteria Standard for Electronic Records Management Software Applications (DoD-5015.2-STD)," November 1997, pp. 7-17.

Unresolved Legal Issues Facing SBA

One reason that many organizations have been cautious in embracing electronic commerce is that they are not yet satisfied that electronic transactions will be treated as legally authentic and binding in court. This is likely to continue until laws and regulations catch up with the technology and become case-tested in the judicial system. Other unresolved legal issues involve conflicts between investigations and privacy, balancing security with access to information, the type of identification needed to determine whether the parties to an electronic transaction are legitimate, and storage of electronic records**.**

Necessity of Contractual Protections for SBA's Use of Electronic Commerce

Until uniform standards and rules are developed to cover electronic transactions, parties to such transactions will have to rely on the language in a contract for an understanding of the legal responsibilities governing their respective actions. At a minimum, a contract should identify (a) a means for authenticating the identity of the contracting parties; (b) a legally recognized form of signature; and (c) secure, reliable commercial records.[2]

With reference to these legal issues, the OIG recommends that:

5) The Office of General Counsel, in consultation with program managers and the Office of the Chief Information Officer, ensure that contractual agreements and related modifications with resource partners and small businesses using electronic means to conduct business with SBA--

- **Define what constitutes a valid electronic identity and signature for each party.**
- **Hold each party responsible for the accuracy of the electronic information it transmits.**
- **Define each party's recourse if the other fails to carry out any part of the agreement.**

---

[2] Sutin, Alan. Roadblocks Stall Electronic Commerce. *New York Law Journal*, July 13, 1998, www.nylj.com.

ORGANIZATIONAL ISSUES

The experiences of other organizations reveal several important lessons-learned that may benefit SBA as it moves toward a paperless office environment:

1. Decide which work processes should be paperless based on solid business analysis, rather than simply on the availability of advanced technology.

2. Strive to have work processes and electronic systems operate seamlessly by integrating databases, hardware, and software programs that currently operate independently of one another.

3. Recognize that human factors are at least as important as technology in implementing paperless business solutions.

Business Analysis

An organization needs to ensure that implementing a paperless office environment makes good business sense. This means first examining business functions to determine (1) whether they need to be performed in the first place and (2) whether any changes to improve business operations lend themselves to technological applications.

Any application of paperless office technology should be preceded by a strategic assessment of how the application supports the organization's plans for product and service delivery. Decision-makers need to consider the ways people work and interact and how underlying work processes could be influenced positively by going paperless. A good example can be found in SBA's Office of Capital Access, which has undertaken the reengineering of work processes as part of its loan modernization effort.

There was a consensus among the many SBA officials we interviewed that a working group of Agency managers should be appointed by the Administrator to make the necessary assessments and to oversee prospective conversions to a paperless environment. Such a central coordination group would ensure that obsolete work processes are not automated, that electronic initiatives are compatible inside and outside the Agency, and that no attempts to create electronic initiatives go forward without giving full consideration to their effect on the rest of SBA and its partners.

The paperless proposals that passed this screening would then undergo the detailed policy and cost evaluations performed by SBA's existing Business Technology Investment Council (BTIC). BTIC thus could be assured that management had considered work processes *before* trying to buy technology, and the Agency could avoid fragmented implementation of electronic initiatives.

Conversion to a paperless environment can be expensive, with benefits difficult to quantify, particularly if an organization attempts to handle everything itself. However, a

major technology firm estimates that it could establish a digital signature environment at SBA—to be used initially with preferred lenders—at a cost of between $75,000 and $100,000. The annual ongoing cost is estimated at $30,000. In addition, SBA would have internal expenses such as validating employee and resource partner identities, employee training, and possible enhanced security. Offsetting the costs are potential—and difficult to measure—savings in paperwork processing, reduced staff time, and consolidated processes.

Work Processes and Information Systems

An important need for organizations making the transition to a paperless environment is the smooth integration of their disparate single-purpose databases and their hardware and software platforms. The multiple databases often found in large organizations need to be integrated to ensure that personnel have access to data that needs to be shared. Otherwise, staff may be forced to rely on proprietary "stovepipe" databases that separate products or programs from each other, create unnecessary bottlenecks, and make data management more complex and costly. An example of an initiative supporting integration is SBA's Digital Signature Technology Policy and Oversight Committee, which seeks to develop a common electronic signature architecture for the entire Agency.

Human Factors

Perhaps the most important organizational issue is the recognition of human factors that, if left unattended, can bring a halt to the most elegant or technologically sophisticated solutions. Our research found that while technological innovations continue to overcome technical systems problems, organizations often underestimate the cultural and human obstacles to success in the paperless office. Moreover, for paperless office initiatives to be embraced by any organization, they must be driven by the managers and users, rather than the technical staff.

What specific steps should an organization follow to become paperless? One of the most ambitious electronic initiatives in the Federal government is the DoD effort to implement a paperless contracting process. The blueprint for accomplishing this calls for--

- Establishing a senior-level steering group,
- Creating incentives for people to exchange information electronically,
- Improving coordination and communication across functional areas,
- Reviewing and eliminating policies and procedures requiring that information be stored on paper, and
- Reviewing statutory requirements for proposed legislative relief from paper creation.[3]

---

[3] Department of Defense, "Blue Print for Paper-Free Contracting Process (Revision A)," September 4, 1997, p. 18.

Based on the organizational issues we have identified, the OIG recommends that:

6) A top-level SBA official with authority over SBA programs, such as the Chief Operating Officer, lead a central coordination group of managers, staff, and technical experts to--

- **Identify any major Agency work processes that should be eliminated or performed by outside parties.**
- **Identify processes that are candidates for electronic initiatives.**
- **Refer the electronic initiatives approved by the group to the Business Technology Investment Council for detailed policy and cost evaluation.**

SBA COMMENTS

The Office of Chief Information Officer and the Office of General Counsel concurred with the report's recommendations. In addition, the Chief Operating Officer indicated her support for the report's findings.

BACKGROUND

The Paperless Office

The world's banking and financial services institutions are undergoing technological changes unparalleled in their history. According to a leading bank that relies on state-of-the-art technology, much of its business in the next two decades will come from customers it does not have today, involve products and services that do not exist today, and be delivered in completely new ways. Likewise, SBA and other organizations—in both the public and private sectors—are gradually moving toward "paperless" methods of conducting business. Much of this movement is spurred by the organizations' need to streamline their operations while sustaining high-quality levels of service despite reductions in staffing and other resources. According to Agency officials, converting to a paperless environment will save SBA money, labor, and time, while improving customer satisfaction and providing new and enhanced services.

For our purposes, an office is defined as having a paperless environment if its work processes are essentially electronic, with minimal required use of paper documents and reduced need for human handling of routine tasks. The purpose is to eliminate the inefficiencies that a paper-based, relatively labor-intensive environment causes, such as errors from duplicative data entry, and to automate routine functions if the benefits of doing so outweigh the costs. The benefits of automation can also occur through the paperless exchange of business documents among organizations, i.e., electronic commerce. Thus, in a paperless office, most but not all information would be transmitted and stored electronically. Nonetheless, "going paperless" requires more than simply installing new computers and software. As will be shown, it can have serious security and legal ramifications and significantly affect both an organization's work processes and its internal culture.

How Electronic Technology Is Evolving

The technological world in which SBA operates is increasingly open. Users have greater access to one another, particularly through the international system of computer networks known as the Internet.[4] This is due in part to greater interoperability, i.e., the ability of diverse electronic systems to communicate with each other through any network. Declining costs also play a major role in widening access, as evidenced by the ability of small businesses to advertise to the world via the Internet at a lower cost than through local newspapers, television, or other media. *For SBA, this means cost-effective opportunities for reaching small businesses and working with resource partners.*

Electronic technology continues to change the way people accomplish their work. It has diminished the need for intermediaries and physical assets, while also erasing

---

[4] The Internet access system that allows millions of computers to connect to thousands of servers is the World Wide Web.

geographical boundaries, particularly in the financial marketplace. At the same time, processes that add no value to the organization can be eliminated or shifted to the customer. For example, one of the world's leading management consulting firms estimates that a customer using a teller costs a bank $1.07, while an automated teller machine (ATM) transaction costs $0.27. If that customer uses the Internet, the cost is $0.01.[5] Clearly, these are powerful incentives for organizations to have users do the work themselves—electronically.

Unfortunately, progress comes at a price. Greater dependence on electronic systems can mean greater vulnerability to "cybercrime" or technical breakdown, particularly if the systems are poorly implemented. As will later be discussed, the very strength of networks—their interconnectedness—is also their greatest weakness.

Private Sector Usage of Paperless Initiatives

According to officials in several large companies, the greatest advantage of going paperless is the savings in money and time, particularly as new uses for advanced technology appear. Some envision prospective borrowers applying for loans electronically at public kiosks, which would replace bank branches over the next 20 years. Although the private sector is eager for the cost savings of a paperless environment, converting to an electronic environment is not always appropriate. For example, officials of two major insurance companies stressed that going paperless should not be viewed as a goal itself, but only as a tool to support organizational objectives, e.g., increasing revenues, reducing staffing and storage costs, accessing documents in a timely manner, reducing errors, and improving goods or services. In other words, electronic conversion requires a compelling business or customer service reason to be cost-effective.

In some cases, the costs of implementing a paperless environment, e.g., training and time away from regular work, may exceed the benefits. Private sector managers we interviewed also noted that a cost-benefit analysis can be difficult to perform because the conversion to a paperless environment is expensive and the benefits are hard to quantify.

SBA's Approach to a Paperless Environment

SBA plans to become a "21st Century Leading-Edge Institution" through centralizing work processes, modernizing technology, and outsourcing portions of programs, including a major part of the Office of Disaster Assistance's loan portfolio. Advanced technology will enable the Agency and its resource partners to continue moving toward electronic lending from origination through servicing, as in the SBAExpress program.

According to SBA officials, the sizable cuts projected in staffing will compel the Agency to make greater use of technology and serve more as a portfolio manager in the future. The Agency will likely perform more oversight functions, such as monitoring preferred lenders and outsourced services, and act as a facilitator to match small businesses with

---

[5] Andersen Consulting. *What's the Value of eCommerce?* www.ac.com/showcase/ecommerce/ecom.

resources. Also, there will be more coordination between SBA and other agencies to ensure that small businesses have access to as many resources as possible.

SBA believes that to continue its commitment to bring the Agency's programs, products, and services to a wider range of small businesses in an efficient and effective manner, it must take full advantage of emerging technologies. This includes using Internet technology, video conferencing, and long-distance learning to ensure the broadest possible access to SBA's programs and services. At the same time, SBA officials caution that electronic initiatives should be viewed as long-term efforts. In the short term, the Agency intends to use both paper-based and electronic methods, particularly for resource partners and small businesses whose operations remain largely dependent on paper.

In order to update its information technology systems for the transition to a paperless office, SBA is focusing on modernizing the following basic components:

- Business lending programs,
- Disaster assistance lending program,
- Accounting functions,
- Non-lending programs (Minority Enterprise Development, Government Contracting, and Surety Guarantees),
- Access to information (decision support, electronic information system, ad hoc query), and
- Productivity enhancement (workflow, Intranet).[6]

A current initiative is to use electronic commerce technology to transmit funds and data between SBA's resource partners and the Agency. SBA is working with the Department of the Treasury and others to use the Agency as a test site to develop this technology for use throughout the Government.

According to SBA officials, the payroll system is likely to become electronic within five years, and billing will be done without human intervention except when there is a problem. Moreover, there have been extensive discussions within the Office of Capital Access concerning the development of paperless office initiatives. For example, the Low Documentation (LowDoc) loan program eventually could become entirely electronic. Agency officials believe that ultimately 75 percent of loan activity in the Section 7(a) guaranteed loan program will be paperless. They also note that, within the Section 504 Certified Development Companies program, the Premier Certified Lender Program (PCLP) ultimately will be electronic. According to one official, the non-PCLP lenders also want to go paperless.

The Agency also has taken steps to implement paperless office initiatives in other programs. The disaster assistance program is creating a paperless application and loan process for home loans, and the micro-lending program is developing ways to transfer electronic information to its intermediaries. In the Office of International Trade, all

---

[6] SBA's Five-Year Revised Strategic Plan (FY1998-FY2002), "Creating Opportunities for Small Business Success (Draft)," June 9, 1998, p. 63.

reporting will eventually be electronic. In the Office of Surety Guarantees, companies in the Preferred Surety Bond program submit their bond information electronically. Finally, in the Investment Division, funding for Small Business Investment Companies is handled electronically, and the reporting function combines electronic and non-electronic means.

Despite such efforts, SBA officials acknowledge that internal administrative processes—such as handling travel documents and requisitions for supplies and services—remain largely paper-based. According to these officials, efforts to go entirely paperless have been stifled by uncertainties about electronic signatures and incompatibility among different information systems. Thus, many documents continue to be printed, approved, and processed manually; some officials advocate greater use of the Agency's Intranet as a possible solution.

SBA and the Emerging Public Key Infrastructure

If current trends continue, SBA will probably conduct much of its business through a Public Key Infrastructure (PKI). As defined by a multi-agency steering committee promoting its use in the Federal Government, PKI is "a combination of products, services, facilities, policies, procedures, agreements, and people that provides for and sustains secure interactions on open networks such as the Internet."[7] A more detailed explanation of PKI is found in the section on security issues.

If properly and economically implemented, PKI is important to SBA because it addresses the issue of public trust in electronic commerce. Despite their growing popularity, electronic transactions do not yet enjoy the same public trust as paper-based transactions. By contrast, a written signature on a paper document is usually considered valid unless later proven otherwise.

In an electronic transaction, the parties need to know that messages are valid (authentication) and that data remains unchanged from its source (data integrity). The sender needs to be certain that the data has been delivered and the recipient needs confirmation of the sender's identity (non-repudiation). Finally, the authorized parties need to be sure that the information can be read only by them (confidentiality). Without such assurances, public acceptance of electronic commerce may be limited, thus minimizing potential efficiencies and cost savings for SBA and its partner organizations.

---

[7] Federal Public Key Infrastructure Steering Committee, "Access With Trust," September 1998, p. 5.

OBJECTIVES, SCOPE, AND METHODOLOGY

Over the next few years, SBA will make greater use of electronic communications and work methods, while relying less on paper-based processes. Despite the enormous efficiencies promised by a paperless environment, the Agency faces numerous security, legal, and work process challenges. Accordingly, the Office of Inspector General (OIG) initiated this inspection as a proactive effort to identify potential problems and to help SBA management successfully make the transition to a paperless environment.

The inspection team conducted extensive library and Internet-based research of private, public, and nonprofit sector organizations' efforts to establish paperless offices. Team members also attended workshops and conferences on banking security, electronic government, and defending cyberspace, as well as a data security roundtable sponsored by the President's Council on Integrity and Efficiency (PCIE). The team interviewed and obtained documentation from key Federal officials at the Social Security Administration, the Department of the Treasury, the Office of Management and Budget, the Federal Deposit Insurance Corporation OIG, the Department of Agriculture OIG, and the Department of Justice.

Because some companies in the private sector appear to be taking the lead in moving toward a paperless environment, team members gathered considerable information about that sector's experiences. The banking and insurance industries in particular were chosen for Internet research and interviews because parts of their business operations—such as accepting applications and providing for customer credit needs and guarantees—are especially relevant to SBA operations. Nonetheless, other industries also proved instructive in terms of the changes that a paperless environment brings to an organization. To encourage frank discussion of sensitive issues, the OIG agreed not to identify the companies interviewed by name. Finally, to obtain perspectives from within the Agency, team members interviewed SBA officials in the offices of Administration, Capital Access, Disaster Assistance, General Counsel, the Chief Information Officer, and the Chief Financial Officer.

As the data were gathered, it became evident that the issues surrounding the implementation of a paperless office logically fell into three functional areas: security, legal, and organizational. Hence, this report focuses primarily on these three areas.

All work on this inspection was conducted between April 1998 and January 1999 in accordance with the **Quality Standards for Inspections** issued in March 1993 by the PCIE.

SECURITY ISSUES AFFECTING SBA IN A PAPERLESS ENVIRONMENT

To protect everything is to protect nothing. –Napoleon Bonaparte

The Basic Problem

If resource and other constraints made prioritizing security needs essential in Napoleon's time, then such limitations are particularly relevant today, as the number of electronic linkages—and potential security breaches—rapidly increase. According to the U.S. General Accounting Office (GAO), "the government's increasing reliance on interconnected systems and electronic data also increases the risks of fraud, inappropriate disclosure of sensitive data, and disruption of critical operations and services."[8] However, to gain the greatest benefits from the electronic exchange of information, agencies such as SBA must take the risk of allowing at least limited access to their systems. The problem is how to balance access with security, without wasting limited financial and human resources.

Security Principles

According to computer security experts in both the private and public sectors, organizations attempting to secure their electronic systems should adhere to the following basic principles:

- Senior management needs to recognize information resources as essential organizational assets.

- The organization should identify the key information assets that require the greatest protection.

- Paying disproportionate attention to one part of a system is likely to result in a false sense of security, not better overall security. For example, encryption by itself does not ensure security. [9]

- No electronic security solution should be considered foolproof.

- An organization cannot stop an attacker; it can only slow him/her down and buy time to detect and react to the attack.

---

[8] General Accounting Office, *"Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk,"* (GAO/AIMD-98-92), p. 2.
[9] Encryption is the transformation of plain text into unreadable text in order to protect it.

- The greatest threats are internal, e.g., employees who are disgruntled or simply inattentive to security procedures.

- Because every security control has a cost, the decision to impose a new control should be based on a careful business analysis of the expected benefits.

In short, effective security means setting priorities by considering the value of the information to be protected, the extent to which such information is at risk, and the cost of safeguards. According to a major management consulting firm, an organization should first identify the most valuable informational assets to ensure efficient use of resources, employee support of security methods, and seamless integration of security with an organization's goals. Without such a prioritization, an organization may inadvertently spend money and effort protecting low value data at the expense of valuable information.

Some prioritization already occurs at SBA. Officials from the business loan program, for example, stated that they inform the Office of the Chief Information Officer (OCIO) what types of information can be released to the public. In addition, the Agency's draft revision of the operating procedure for automated information systems security requires sensitivity determinations for all computerized data. Nonetheless, it is unclear to what extent program managers, attorneys, and other knowledgeable staff *systematically* coordinate their priorities to ensure that *only* the most valuable information receives the highest level of protection. Moreover, as programs change, SBA officials are likely to need to redefine which information is valuable.

External Threats

Even with the above in mind, balancing access with security is difficult when some of the problems SBA faces originate outside of the Agency. For example:

- Because of competitive pressures, few software developers adequately research security problems before bringing products to market, thus increasing the odds of complications later. For example, one prominent technology firm introduced Internet software containing a major security defect that rudimentary research could have detected. Some technologists contend that most network software is designed for maximum utility, with security being an afterthought.

- Codes can be broken. For example, a private foundation needed only 54 hours and less than $250,000 in hardware to crack a messaging encryption standard to which the Federal Government had long pressed industry to limit itself. Moreover, intruders known as hackers sometimes work together from different locations to penetrate information systems. Although encryption techniques continue to improve, so does the sophistication of attacks.

- Protecting sensitive data at one's own site is not enough. An organization must also understand the level of security at the entities with which it conducts business. The other party's weak link can become the weak link of everyone who deals with it.

Unfortunately, there is currently no clear consensus on how to handle sensitive data. Some experts believe that it can be sent over public networks as long as it is encrypted. Others, mindful that any internal network connected to the Internet is accessible to outside intruders, believe such data should be kept off networks altogether. Nevertheless, security procedures for handling the external environment are available. To establish a high level of security, SBA separates its public access network from its private internal network by firewalls, i.e., combinations of hardware and software placed between two networks designed to block unauthorized access. Moreover, according to a draft operating procedure, the Agency requires that corporate or sensitive data transmitted over the Internet to approved destinations be encrypted.

Another procedure is to use software "patches" to update an information system's security when a new threat is identified. Despite patches' usefulness, one Federal technology official estimated that 70 percent of government network administrators were not applying the latest patches to update their agencies' electronic security. Moreover, the use of patches has limitations. For example, having security experts break into a system and then patch the vulnerability can occur too late, thus leaving hackers a step ahead. Hackers could monitor security patch announcements and then exploit targeted machines before the patches can be installed. There is even the possibility that downloading patches to solve software flaws could harm security because of rogue organizations posing as patch vendors. In an interconnected electronic world, impersonating others is not difficult if security is poorly implemented.

Internal Threats

According to the Federal Reserve, various security surveys have found that the majority of attacks on private networks come from internal sources.[10] Others estimate that 80 to 95 percent of all security incidents result from an insider attack.[11] This is particularly troubling because an organization's personnel, including consultants, are likely to have access to critical systems as well as detailed knowledge of the organization's practices. In one case, an Air Force staff sergeant used the password of another employee as part of his scheme to embezzle over $435,000.

Sometimes an internal threat results from naivete or carelessness instead of malicious intent. According to experts, computer users have become too trusting, using the same

---

[10] Federal Reserve System, "Sound Practices Guidance for Information Security for Networks" (paper presented on April 23, 1998, at the Bank Administration Institute's Electronic Banking Security Conference), p. 9.

[11] Marcella, Albert J. Jr., Larry Stone, and William J. Sampias. *Electronic Commerce: Control Issues for Securing Virtual Enterprises*. Altamonte Springs, FL: The Institute of Internal Auditors, 1998, p. 95.

passwords to enter both secure and non-secure computer sites, thus making it easier for thieves to steal the passwords. Another all-too-common problem is "social engineering," in which a hacker tricks someone inside an organization into revealing secret codes. The intruder may pose as a new employee or help desk person to obtain passwords or other confidential employee data that can be used to break into an information system.

Accordingly, the most important lesson from security experts is that if an organization ignores the human element, even the most sophisticated encryption, firewalls, and PKI protections may be rendered useless. Making the necessary adjustments in the organizational culture is at least as important as selecting the right technology. It is critical, therefore, for management to (1) identify the information requiring the highest level of protection, particularly in terms of the risk of loss relative to the cost of safeguards, and (2) ensure that proper internal security practices are fully understood and closely followed.

Security on the Internet

The Internet presents special security problems. Because the method of sending e-mail over the Internet was not designed with security in mind, "sniffing" software can intercept transmitted data, enabling intruders to steal user identification, unencrypted passwords, and entire messages and files. Such intruders can then masquerade as the authorized users to commit fraud and other crimes. As Internet browsers become more complex and powerful, software flaws are more likely, resulting in potentially greater vulnerabilities.

There are several ways to combat these vulnerabilities and protect Internet transmissions. As mentioned earlier, software patches can correct known security deficiencies, such as a widely reported defect in a Microsoft office suite that exposed passwords and other sensitive data originating from users' computers. Information sent over the Internet can be encrypted or scrambled, thus rendering it useless to those intercepting it. Sections of a network can be separated, e.g., Internet access operations can be on a system different from the agency's main computer system.

Nonetheless, protecting any organization from outside electronic attack requires that Web servers, firewalls, and encryption/authentication systems interact in a smooth and precise manner. Software systems are often large and complex, and a single flaw can give an attacker entry into an otherwise secure system. Accordingly, the lingering public uncertainties about the Internet are hastening the implementation of the Public Key Infrastructure, whose underlying technology has been developed by private industry and is being marketed and used commercially. In addition, over 20 Federal pilot projects are testing various aspects of the technology. The major challenge is for the infrastructure to satisfy the needs of vastly different users.

Public Key Infrastructure (PKI): The Basics

PKI is designed to ensure secure transactions on open networks such as the Internet. To

address security concerns, PKI employs a data item called a digital signature, which is used with a digitally encoded message to prove the sender's identity and the message's integrity. It is important to note that a digital signature is not simply a digitized handwritten signature, a person's typed name, or a personal identification number.

To ensure the digital signature's uniqueness, the sender and recipient each have a public (published) key and a private (secret) key, i.e., a digital representation of a very large number. When a sender uses the *private* key to sign an electronic message digitally, anyone knowing the sender's corresponding *public* key can verify the sender's signature.

To enable the keys to work, PKI requires a trusted third party—known as a certification, or certificate, authority (CA)—to vouch for the sender's identity. The CA issues a digitally signed message—called a digital certificate—binding the sender's identity to his/her public key. The certificate is maintained by the CA and signed using the CA's private key.

Of course, someone needs to certify an individual's identity to the CA so that the CA may issue a digital certificate in the first place. An entity called a registration authority performs this function; it may or may not be part of the CA.

In some ways, a digital certificate resembles a credit card or driver's license—an item issued by an organization having information about the user and able to verify the item's authenticity. However, as in the case of these two items, PKI needs to ensure that certificates have a limited lifetime and can be revoked.

The practical use of digital certificates is moving closer to reality. Recently three leading security technology firms collaborated with banks in a pilot project to establish the interoperability of participating banks' digital signature technologies. In 1999, a global bank became the first such institution to successfully provide digital certificates to its corporate clients. SBA has served on the multi-agency steering committee promoting PKI within the Federal Government. Internally, the Agency has begun defining the requirements for implementing digital signature technology. However, implementation in any Federal agency will require resolving a number of difficult issues, including those presented below.

PKI Accountability and SBA

Authenticating identity traditionally has been an inherently governmental function; PKI, however, will rely largely on security solutions developed by private industry. Accordingly, it will depend on honest and competent CAs and registration authorities. A variety of organizations are preparing to become CAs, including the American Bankers Association (ABA), which in 1998 announced plans to become a CA for the financial services industry. The ABA also encouraged banks and other financial services companies to become CAs, whether solely for their own customers or to provide services to external entities.

The potential for many entities to become CAs raises a number of serious accountability questions. For PKI to work, a CA must be recognized as trustworthy. In theory, a drug cartel could operate a CA because currently any organization can issue digital certificates. Even with a legitimate CA, there is the issue of how reliant parties such as SBA could ensure that the CA was being diligent. For example, the Agency would need to be confident that a CA would cancel digital certificates whenever employees left SBA and, conversely, that all cancelled digital certificates would be kept available for accountability, evidentiary, and documentation purposes. Finally, there are no guarantees that CAs used by other parties will perform honestly or efficiently.

Perhaps the most fundamental accountability problem is not the security of information but, instead, the veracity of the information itself. What assurance does a CA or registration authority have that the underlying personal information upon which digital certificates are based is accurate? CAs and/or registration authorities might rely on databases whose information has not been verified. Moreover, the recent increase in identity fraud suggests that such crimes may not require great sophistication on the criminal's part. Thus, organizations such as SBA face the irony of advanced technology being used to protect false information—the electronic equivalent of a bank safeguarding counterfeit currency.

Given the uncertainties about CAs, registration authorities, the information backing digital certificates, other organizations' level of security, and, as discussed later, the evolution of electronic commerce law, how can SBA protect its interests? Major insurance companies grappling with such uncertainties believe that *contractual agreements* among parties become more important as electronic commerce evolves. They suggest that the reliant organizations have a legal contract that clearly identifies the trusted third party's responsibilities and liabilities.

Another accountability issue is whether a digital certificate should contain so much information that it becomes a universal identifier similar to a Social Security number. If so, what would be the trade-off between administrative convenience and the vulnerability posed by criminals needing only one security breach to obtain a great deal of sensitive information? And would the CA and/or SBA be held liable for the consequences of such a breach?

PKI and Privacy

Privacy is of paramount importance in establishing a trusted and secure paperless environment. Without adequate protections, the enormous benefits of electronic commerce may not be fully realized due to many potential users' natural reluctance to risk their privacy and organizations' fear of lawsuits stemming from the inadvertent release of confidential information. Although technology has changed dramatically, fundamental principles of privacy remain the same.

- Individuals must be able to
--find out what information is held about them,

> --prevent personal information from being used illegally, and
> --correct erroneous information.

- Organizations receiving personal data must
  --assure the reliability of the data for its intended use, and
  --take precautions to prevent misuse of the data.

An evolving Federal effort likely to affect SBA's handling of PKI privacy issues is the General Services Administration's (GSA) Access Certificates for Electronic Services (ACES) initiative. According to GSA, ACES digital certificates are not intended to serve as a single certificate for all government purposes but will support agencies' activities that require identification of a person. Nonetheless, by delivering public key certificates to the public, the ACES initiative seeks to evaluate the feasibility of a uniform identity certificate to promote interoperability among agencies.

Accordingly, privacy advocates worry that ACES would have only a few large registration authorities with similar core identifier elements. To avoid centralization of data about an individual's identity and activities, these advocates prefer many diverse registration authorities. In addition to such decentralization, they argue for multiple certificates to cover different purposes and information practices, ensuring that the information collected is limited to the amount needed to complete a transaction.

It is not clear whether ACES will become the digital standard for the Federal Government or whether new legislation will restrict the contents of digital certificates. If neither occurs, agencies such as SBA may have to choose between two types of digital certificates. The first would provide complete information about an individual and offer administrative simplicity. Unfortunately, it could create the public appearance—if not the reality—of too much information vulnerable to internal theft or misuse. The other type would be limited to the information necessary to complete specific types of transactions, thus minimizing the amount of information at risk. However, this could also impose substantial administrative complications in maintaining different certificates for different purposes.

Internal Security Policies and Procedures

According to both private and public sector officials, choosing and installing new technology are the easy parts of enhancing computer security. Establishing and enforcing appropriate policies and procedures are by far the most difficult aspects.

SBA recently drafted a revision of its Standard Operating Procedure (SOP) for information security that includes the following:

- Protecting passwords by administrative, physical, and technical security controls to prevent unauthorized disclosure or misuse, such as changing employees' passwords at least once every six months.

- Determining the sensitivity of data contained in automated information systems on a regular basis.

- Keeping sensitive information relating to businesses or individuals doing business with SBA off its Web servers.

Nonetheless, private sector managers noted that simply establishing policies and procedures is not enough. Employees need to fully understand their responsibilities and the penalties for not carrying out those responsibilities. For example, a major insurance company ensures that all security policies—such as not sharing passwords—are clearly defined and widely disseminated. A major bank ensures that each employee has at least two passwords that are changed every 30 days. It also informs its employees that sharing a password will result in termination of employment and that employee transactions will be monitored to ensure that security procedures are followed.

Unfortunately, PKI presents special problems. For example, what happens if an employee loses his/her private digital signature key? Unlike the case of credit cards, there is no Federal law capping liability for such a loss. And what happens if someone else uses the digital signature key? Some SBA officials believe that the employee issued the key must be held responsible because he/she was entrusted with it in the first place. Others believe strict penalties would not be enforceable because the circumstance would resemble the limited liability of a lost credit card. Regardless of the extent to which employees are held responsible for their actions, the Agency will need the ability to revoke keys quickly after a loss or security breach.

According to the multi-agency steering committee promoting PKI, agencies need to help establish a liability structure that balances the interests of users and service providers such as CAs. However, due in part to the lack of case law in this area, the committee does not recommend a specific liability policy. Although some security experts believe that the issue of liability may be solved by two-device authentication, i.e., any combination of passwords, digital certificates, hardware tokens, "smart" cards, or biometric devices (such as fingerprint reading), this still does not address the employee's responsibility if *both* devices are lost.

Finally, organizations can overdo security procedures, resulting in unintended consequences. For example, if employees perceive that complex security procedures are too onerous and unnecessarily restrict their work, they may simply circumvent or ignore them.

RECOMMENDATIONS

Recommendation 1. To conserve scarce Agency resources, the OIG recommends that the Chief Operating Officer require that each program, in consultation with the Office of the Chief Information Officer and the Office of General Counsel, identify the types of data requiring the highest level of security and privacy safeguards.

Recommendation 2. **To protect the Agency's interests, the OIG recommends that the Office of General Counsel, in consultation with the Office of the Chief Information Officer, develop contracts applicable to any certification authority or registration authority the Agency might use in a Public Key Infrastructure. Such contracts would identify--**

- **Each certification authority's and/or registration authority's transaction and security responsibilities,**
- **Each certification authority's and/or registration authority's liability for failure to complete an electronic transaction, and**
- **Each party's recourse if it performs a transaction based on the other's false or inaccurate information.**

Recommendation 3. **To allay privacy concerns and limit the exposure of confidential information, the OIG recommends that the Office of the Chief Information Officer, in consultation with the Office of General Counsel, limit future digital certificates to the minimum information necessary to complete Agency electronic transactions.**

Recommendation 4. **To help minimize the likelihood of internal security breaches in an increasingly paperless environment, the OIG recommends that the Office of the Chief Information Officer and the Office of General Counsel jointly develop a concise notice for periodic display on computer screens to remind Agency employees and contractors of--**

- **Their basic information security responsibilities,**
- **The penalties for failure to carry out those responsibilities, and**
- **The fact that using Agency information systems constitutes acceptance of those responsibilities and penalties as well as consent to searches by law enforcement organizations.**

LEGAL ISSUES AFFECTING SBA

Desirable Legal Characteristics of a Paperless Environment

Any organization planning to establish a paperless office environment should first address a number of legal issues, including the authentication of documents and transactions, the possession of a documentable record trail, the admissibility of evidence regarding digital signatures, and the storage of electronic information. Fortunately, there are outside organizations that can provide some guidance on creating the necessary legal infrastructure to make a successful transition to a paperless office.

The National Conference of Commissioners on Uniform State Laws, which is responsible for developing laws on financial payments and other paper-based commerce, is leading the effort to create a statute for electronic commerce. It is attempting to obtain ratification by all states of its draft bill, the Uniform Electronic Transactions Act, by the year 2000. The intent is to establish standards that will prevent conflicting legal rulings among different states. More specifically, the Act seeks to achieve the following:

a) Facilitate and promote commerce and governmental transactions by validating and authorizing the use of electronic records and electronic signatures.
b) Eliminate barriers to electronic commerce and governmental transactions resulting from uncertainties relating to writing and signature requirements.
c) Simplify, clarify and modernize the law governing commerce and governmental transactions through the use of electronic means.
d) Permit the continued expansion of commercial and governmental electronic practices through custom, usage, and agreement of the parties.
e) Promote uniformity of the law among the states (and worldwide) relating to the use of electronic and similar technological means of effecting and performing commercial and governmental transactions.
f) Promote public confidence in the validity, integrity, and reliability of electronic commerce and governmental transactions.
g) Promote the development of the legal and business infrastructure necessary to implement electronic commerce and governmental transactions.[12]

In short, the draft Uniform Electronic Transactions Act provides procedures to enable electronic commerce transactions. To ensure the uniform acceptance of electronic transactions and communications, the Act's scope includes

a) Attribution of an electronic record to a person,
b) Accuracy of information,
c) Retention of electronic records,
d) Legal recognition of electronic signatures,
e) Formation of contracts for electronic records,

---

[12] National Conference Of Commissioners On Uniform State Laws, "Uniform Electronic Transactions Act (Draft)," January 29, 1999, p. 17.

f) Admissibility in evidence, and
g) Interoperability capability.[13]

Current Status Of Relevant Laws And Regulations

The 105th Congress passed a substantial amount of electronic commerce-related legislation, including a bill recognizing electronic signatures, and the current session may see the introduction of additional bills addressing encryption and consumer privacy and protection.

The Government Paperwork Elimination Act of 1998 requires Federal agencies to recognize electronic signatures and make Federal forms available online during the five-year period beginning in 1998.[14] The public will be able to use the Internet to access Federal forms and electronically submit them to Federal agencies using electronic signatures. The law enables Federal agencies to use electronic signatures and ensures that such signatures will not be denied the same acceptability and validity as written signatures.

The Act's recognition of electronic signatures appears consistent with an earlier Comptroller General's ruling on the issue. In 1991, the Comptroller General declared that Federal agencies could create valid obligations electronically.[15] Despite the Comptroller General's ruling and the passage of the Government Paperwork Elimination Act, some businesses have been cautious in adopting the use of electronic signatures due to the lack of legal precedent. Nevertheless, SBA is moving toward meeting the Act's provisions by defining the requirements for implementing electronic signature technology.

Even though the above legislation is in place, at present the legal authority for disposition of certain types of electronic records is in a state of flux. In 1997, a U.S. District Court judge declared "null and void" the National Archives and Records Administration's (NARA) edition of General Records Schedule (GRS) 20, Electronic Records, which provided guidelines for the disposition of certain types of electronic records.[16] The judge's order, presently on appeal, was in response to a lawsuit filed by Public Citizen and others challenging the Federal Government's ability to destroy records. Currently an information technology disposition schedule is being developed to replace GRS 20.

In November 1998, NARA generally endorsed a standard for electronic records management developed by the Department of Defense (DoD).[17] In its endorsement,

---

[13] National Conference of Commissioners on Uniform State Laws, "Uniform Electronic Transactions Act (Draft)," January 29, 1999, pp. 17-49.
[14] Government Paperwork Elimination Act of 1998.
[15] Comptroller General Decision B-245714, issued December 13, 1991 (71 C.G. 109), also available in 1991 WL 315248 (C.G.)
[16] National Archives and Records Administration News Release, "Court Enables National Archives to Proceed with Electronic Records Plans," September 30, 1998, pp. 1-2.
[17] National Archives and Records Administration News Release, "National Archives Endorses Defense Department Standard as Basis for Effective Electronic Records Management," November 19, 1998, p. 1-2.

NARA declared that DoD's standard complied with the requirements mandated by the Federal Records Act for the management of electronic records. This standard provides a baseline for Federal agencies by specifying that records management software perform the following functions:

- Assign a unique, computer-generated identifier to each record.
- Treat electronic mail messages that have been filed as records, including attachments, as any other record.
- Provide for viewing, saving, and printing lists of records (regardless of media) based on record profiles.
- Identify records that can be sent to a repository for storage.
- Notify authorized individuals when a record is eligible for destruction and destroy it after their approval.[18]

Finally, the Computer Fraud and Abuse Act and the general fraud statute (Title 18, USC) cover the misuse of computer systems through either negligence or criminal intent. However, according to SBA's legal staff, there is nothing specific in the Agency's regulations that address this type of crime, although SBA is taking steps to govern Internet use by Agency employees.

SBA's Internet Policy

To help prevent misuse of its data and computer systems, SBA issued an Internet/Intranet policy for Agency employees, effective October 28, 1998. According to the policy's guidelines--

- Already-existing SBA policies, which apply to employee conduct in other circumstances, may also apply to conduct on the Internet. This includes, but is not limited to, policies on intellectual property protection, privacy, misuse of SBA assets or resources, sexual harassment, information and data security, and confidentiality.

- Information on SBA's Internet service is an SBA record, which may be disclosed under the Freedom of Information Act (FOIA). Disclosure determinations on information, including possibly withholding confidential and proprietary information, will be in accordance with SBA's disclosure policy and FOIA. This information may be protected by the Privacy Act, which generally prohibits disclosure of information kept in any SBA Privacy Act system of records unless FOIA requires disclosure.[19]

---

[18] Department of Defense, "Design Criteria Standard for Electronic Records Management Software Applications (DoD-5015.2-STD)," November 1997, pp. 7-17.
(See http://jitc-emh.army.mil/recmgt/#standard)
[19] Small Business Administration Policy Notice, "SBA Internet/Intranet Policy," October 28, 1998, pp. 1-2.

Unresolved Legal Issues Facing SBA

The following external issues are likely to have a bearing on SBA's use of electronic commerce.

Investigations and Privacy. A warrant to search a suspect's computer files may require the government to obtain access to computer files and information, e.g., the transactional habits of Web users, of individuals who are not targets of the investigation. Laws such as the Electronic Communications Privacy Act specify how to conduct such searches. Moreover, to assist Federal agents and attorneys with this emerging area of the law, the Department of Justice issued guidelines for searching and seizing computers in 1994 and supplemented the guidelines in 1997 and 1999. Complicating matters is the fact that privacy principles from the 1970s remain prevalent today even though the technology has created additional privacy dilemmas. Although applicable to the analysis of electronic information, the Privacy Act of 1974 is based on a paper records system. Future legislation may need to further clarify privacy rights and responsibilities in an electronic environment.

Balancing Security with Access to Information. Organizations must ensure that electronic information is reliable and secure. According to a 1997 report by the President's Commission on Critical Infrastructure Protection, the nation's banking and finance infrastructure is vulnerable to attacks by criminals, inside and outside of organizations, who gain unauthorized access to computer systems and data. To protect proprietary and confidential records, organizations such as SBA can use encryption to make important data unreadable without a decryption key. However, law enforcement officials fear that criminals will use the same encryption technology to commit crimes and avoid detection.

The Type of Identification Needed to Determine Whether the Parties to an Electronic Transaction Are Legitimate. As referred to elsewhere in this report, there are concerns as to how many identifiers, e.g., digital certificates, should be used to authenticate identity. If an individual only has one identifier, for example, the system might be easily compromised if that identifier were lost or stolen. On the other hand, people are likely to resist electronic commerce initiatives if they are required to have separate identifiers for many different purposes such as banking, payment of taxes, or small business assistance. Whether one identifier or several identifiers are used, the parties in an electronic transaction must be able to authenticate identity to ensure the reliability and accuracy of electronic transactions.

Electronic Records as Evidence in a Court of Law. Computer communications, such as e-mail and electronic transactions, are creating a new form of evidence, with all the attendant problems in a court of law, e.g., personal responsibility for content, privacy, and evidentiary concerns. In addition to doubts about electronic communications, there are conflicting views concerning the validity of electronic copies of paper documents as evidence. Nevertheless, legal experts have expressed confidence that, as electronic

evidence is increasingly used in court, judges are likely to become more willing to accept it as long as it is deemed reliable from a technical standpoint, e.g., it has not been tampered with.

Storage of Electronic Records. SBA's responsibilities regarding the storage of information are the same in a paperless office as they are in a paper-based office—the Agency must document and store official information in an efficient and secure manner. One problem is determining what constitutes official electronic information in, for example, e-mails. Another problem is how to store long-term electronic records as the technology changes; today's storage medium could be obsolete tomorrow, rendering electronic documents difficult to retrieve or, at worst, unusable. In such a situation, SBA could be held liable to the same extent as if Agency records were lost or destroyed.

In conclusion, many organizations have been cautious in embracing electronic commerce partly because they are not yet satisfied that electronic records will be secure, available, legally authentic, and binding in court. This is likely to continue until laws, regulations, and records management practices catch up with the technology and become case-tested in the judicial system.

Necessity of Contractual Protections for SBA's Use of Electronic Commerce

At present, there is a measure of confusion as to what type of contract is needed to conduct business in a paperless office environment. States have generally been the laboratories for electronic commerce laws and, as a result, non-uniform standards are being developed. For example, Florida, Minnesota, Utah, and Washington have enacted comprehensive legislation to cover a wide range of issues regarding the use of digital signatures in electronic commerce. In contrast, Arizona, California, Indiana, and North Dakota have essentially limited their legislation to the use of digital signatures for documents submitted electronically to the state government. With each state enacting its own law, significant confusion can occur concerning the allocation of liability for the parties involved in interstate electronic transactions.

Until uniform standards and rules are developed to cover electronic transactions, parties to such transactions will have to rely on the language in a contract for an understanding of the legal responsibilities governing their respective actions. Some computer law experts recommend that the parties to a contract ensure that provisions specifically addressing electronic transactions are fully understood and included. At a minimum, a contract should identify (a) a means for authenticating the identity of the contracting parties; (b) a legally recognized form of signature; and (c) secure, reliable commercial records.[20]

---

[20] Sutin, Alan. Roadblocks Stall Electronic Commerce. *New York Law Journal*, July 13, 1998, www.nylj.com.

RECOMMENDATION

Recommendation 5: The OIG recommends that the Office of General Counsel, in consultation with program managers and the Office of the Chief Information Officer, ensure that contractual agreements and related modifications with resource partners and small businesses using electronic means to conduct business with SBA--

- **Define what constitutes a valid electronic identity and signature for each party.**
- **Hold each party responsible for the accuracy of the electronic information it transmits.**
- **Define each party's recourse if the other fails to carry out any part of the agreement.**

ORGANIZATIONAL ISSUES AFFECTING SBA

In the words of one SBA manager, the purpose of technology for any organization is "to get the right information to the right person at the right time in the right place and in the right format." Reaching that ideal, however, will require more than simply linking computers. The experiences of other organizations reveal several important lessons-learned that may benefit SBA programs as they move toward a paperless office environment. In particular, there are three steps that organizations must take at the start:

1. Decide which work processes should be paperless based on solid business analysis, rather than simply on the availability of advanced technology.

2. Strive to have work processes and electronic systems operate seamlessly by integrating databases, hardware, and software programs that currently operate independently of one another.

3. Recognize that human factors are at least as important as technology in implementing paperless business solutions.

Business Analysis

An organization needs to ensure that implementing a paperless environment makes good business sense. This means first examining business functions to determine (1) whether they need to be performed in the first place and (2) whether any changes to improve business operations lend themselves to technological applications. Just as technology alone should not be the driving force behind change, an organization should not expect to merely apply new technologies or strategies to old business processes.

Instead, any application of paperless office technology should be preceded by a strategic assessment of how the application supports the organization's plans for product and service delivery. Decision-makers need to carefully consider the ways people work and interact and not just rethink the business processes. An assessment of how underlying work processes can be influenced positively by going paperless should then follow. A good example can be found in SBA's Office of Capital Access, which has undertaken the reengineering of work processes as part of its broader loan modernization effort.

Officials at insurance companies we interviewed also advocated a cautious, "go slow" approach to implementing technological solutions. Moreover, some of these officials believe that for certain applications the best alternative may be to continue use of paper-based transactions.

To make the necessary assessments, there was a consensus among the many SBA officials we interviewed that a working group of Agency managers should be appointed by the Administrator to make the necessary assessments and to oversee prospective conversions to a paperless environment. The head of the group—ideally the Chief

Operating Officer—could coordinate input from other members and serve as the leader in planning paperless office initiatives. Although Central Office officials would likely dominate the group, field staff representation would provide a nationwide perspective.

Such a central coordination group would undertake the business analyses for paperless proposals, including any new Internet presence planned by an SBA office. The group would ensure that obsolete work processes are not automated, that electronic initiatives are compatible inside and outside the Agency, and that no attempts to create electronic initiatives go forward without giving full consideration to their effect on the rest of SBA and its partners.

The paperless proposals that passed this screening would then undergo the detailed policy and cost evaluations performed by SBA's existing Business Technology Investment Council (BTIC). BTIC thus could be assured that management had considered work processes *before* trying to buy technology, and the Agency could avoid fragmented implementation of electronic initiatives.

As noted earlier, conversion to a paperless environment can be expensive, with benefits difficult to quantify, particularly if an organization attempts to handle everything itself. However, a major technology firm estimates that it could establish a digital signature environment at SBA and act as a CA—initially with preferred lenders—at a cost of between $75,000 and $100,000. This would include creation of Web pages, provision of several thousand digital certificates, and training of some SBA staff who in turn could train others. After the first year of operation, the annual ongoing cost for maintaining directories and browsers is estimated at $30,000. In addition, SBA would have internal expenses such as validating employee and resource partner identities, employee training, and possible enhanced security. Offsetting the costs are potential—and difficult to measure—savings in paperwork processing, reduced staff time, and consolidated processes.

Work Processes and Information Systems

An important need for organizations making the transition to a paperless environment is the smooth integration of their disparate single-purpose databases and their hardware and software platforms. The multiple databases often found in large organizations need to be integrated to ensure that personnel have access to data that needs to be shared. Otherwise, staff may be forced to rely on proprietary "stovepipe" databases that separate products or programs from each other, create unnecessary bottlenecks, and make data management more complex and costly.

The experience of a major global bank provides an instructive example. The bank found that its old way of doing business meant that each product in every country it served operated with virtual autonomy, making it difficult to access other products of the bank from around the world. This was expensive and did not provide customers with the customization to meet their needs. Also, the operation in each country and the related products employed a model that banks have used for years: a front office (the branch

24

network and sales), a middle office (customer service and loan approvals), and a back office (statement preparation, loan servicing, and payments processing). Each office functioned independently.

These disparate operations began to disappear as the bank developed a standardized global technology platform and integrated the front, middle, and back offices. The bank also adopted an open architecture, adding system flexibility as the offices consolidated. This will enable the bank to reduce from 50 to 10 the number of data centers needed to support its business.

As in the case of the bank, SBA officials recognize that maintaining dissimilar hardware and software programs within the Agency can create interoperability problems across programs and functional areas. Isolated pockets of automation and different systems for different programs tend to separate departments and prevent the linking of SBA products and services to best meet customer needs. Some offices in the Agency have recognized this problem and proposed solutions. An OCIO report acknowledged the importance of integrating separate databases, hardware, and software platforms.

> The number one rule of data management is that data is a corporate resource. . . . The creation of **enterprise databases**, shared by all and owned by none, requires a fundamental shift. . . . Making the shift to an **enterprise data environment** requires integrated methodologies, adherence by all to rigorous methods and standards and a strong data management function with agency-wide influence. . . . The importance of **enterprise data** cannot be over emphasized.[21]

Similarly, officials in SBA's Office of the Chief Financial Officer have recognized the importance of an integrated financial management system.

> We envision a group of user-friendly systems that have the same "look-and-feel," contain standardized and accurate information, and communicate electronically in order to enhance the financial and programmatic management capacities of the Agency.[22]

An example of an initiative toward this end is SBA's Digital Signature Technology Policy and Oversight Committee, which seeks to develop a common electronic signature architecture for the entire Agency. Similar Agency-wide approaches can help integrate stovepipe databases, hardware and software platforms.

---

[21] Small Business Administration, Office of the Chief Information Officer, S*trategic Information Technology Vision*, October 1998, p. 6.
[22] Small Business Administration, Office of the Chief Financial Officer, *Financial Systems Vision*, November 1998, p. 12.

Human Factors

The third, and perhaps most important, organizational issue to be addressed before the implementation of paperless office initiatives is the recognition of human factors that, if left unattended, can bring a halt to the most elegant or technologically sophisticated solutions. Our research found that while technological innovations continue to overcome technical systems problems, organizations often underestimate the cultural and human obstacles to success in the paperless office. As one SBA official noted, the "low-tech issues can scuttle high-tech solutions," meaning that failing to address the more basic human issues, e.g., resistance to change, inattention to security procedures, or fear of job loss, can prevent the successful implementation of high-tech solutions. Moreover, for paperless office initiatives to be embraced by any organization, they must be driven by the managers and users, rather than the technical staff. Users need to know that they have input into the initiatives and that their buy-in is critical to the success of the paperless office.

Still, resistance to change is likely, particularly when people have fallen into familiar and comfortable ways of performing their jobs. According to a principal at a firm that follows the document-imaging market, "You can't force a new process and a new technology on people. That will overwhelm them."[23] To win support for a new technology, organizations need to show users how the change can make their jobs more productive and satisfying.

One example of a paperless initiative from the private sector that benefited both users and the organization is that of a major airline's maintenance operations division, which replaced an elaborate paper and microfilm-based system with a completely electronic one. The airline had been using microfilm readers/printers for its mechanics to view and print maintenance reference documents for the airline's fleet of planes. The primary business reason for the electronic conversion was the need to reduce the amount of time mechanics took to access the reference data during the repair process. Once implemented, the new electronic system dramatically reduced the number of data-related errors while also reducing the time and effort required by clerical staff to keep records current. Anecdotal observation showed that the time it took a mechanic to access information was reduced on average from 15 minutes to 30 seconds. Mechanics now spend less time searching reference manuals and have more time to actually repair planes, thus benefiting the mechanics, the airline and, not incidentally, the flying public.

Another example of a paperless initiative that benefited both users and the organization is from one of the country's largest real estate firms, which implemented a specialized software package for filling out the forms necessary in real estate transactions. This software enables the administrative staff to scan the appropriate forms and complete them on a personal computer. This allows for easy indexing and retrieval, while increasing the

---

[23] Sherman, Erik. Paperless Office Still a Goal, But Reality Remains Elusive. *MacWeek Solutions,* June 17, 1996, p. 3.

staff's efficiency and productivity. Such employees can now devote time to the more productive aspects of transactions, thus benefiting themselves, their firm, and their customers.

Some officials interviewed noted that the application of technology to the workplace is often associated with the loss of jobs. However, this is not always the case, as a major insurance company found when it implemented a paperless initiative. Originally, 120 people were targeted for possible layoffs but were instead assigned to other jobs. Moreover, as one SBA official has pointed out, new technology can create new jobs as older functions are changed or eliminated. The Internet, for example, has created a need for "cybrarians," people who organize electronic data like librarians. This function did not exist before the application of Internet technology. In short, Agency employees need to know that although job functions may change, new technology does not automatically mean job loss.

Based on other organizations' experience, the successful implementation of paperless office initiatives at SBA is likely to be evolutionary rather than revolutionary. And even when enterprise-wide solutions are chosen, the best option is often for incremental implementation. The Agency has already taken this course with its use of pilot programs to test electronic applications, such as with the SBA*Express* and *LowDoc* business loan programs.

What specific steps should an organization follow to become paperless? One of the most ambitious electronic initiatives in the Federal Government is the DoD effort to implement a paperless contracting process. The blueprint for accomplishing this calls for--

- Establishing a senior-level steering group,
- Creating incentives for people to exchange information electronically,
- Improving coordination and communication across functional areas,
- Reviewing and eliminating policies and procedures requiring that information be stored on paper, and
- Reviewing statutory requirements for proposed legislative relief from paper creation.[24]

These generic steps should be the basis for any organization seeking to carry out paperless initiatives.

Examples of Governmental Paperless Office Initiatives

There are numerous examples of agencies already using paperless office systems to deliver government products or services. Two of the most popular and effective electronic delivery channels for government information and services are public kiosks and World Wide Web home pages. SBA has a comprehensive Web site and envisions

---

[24] Department of Defense, "Blue Print for Paper-Free Contracting Process (Revision A)," September 4, 1997, p. 18.

using self-service kiosks to provide information and technical assistance to small business entrepreneurs.

Kiosks are well suited for service transactions because private telecommunications networks have provided their security. They can provide citizens with "one-stop shopping" for government information and services, particularly when placed in malls, government office buildings, and other public locations. Moreover, several agencies can utilize and share the cost of a kiosk. Here are two examples of kiosk applications:

- ServiceOntario, a network of self-service kiosks installed throughout the Canadian province, has enabled residents to obtain key motor vehicle information and services at more convenient times and locations. The program began as a pilot but quickly expanded to over 60 kiosks that now allow citizens to perform such functions as renewal of vehicle registrations, payment of court and parking fines, and ordering of customized license plates. The program has received overwhelming support from the public, with 94 percent of users rating the service "easy to use and enjoyable."

- The Colorado Department of Labor has converted eight unemployment offices around the state from traditional counter-based operations to sites supported by computer kiosks. At these locations, citizens can complete applications and search for information directly from the kiosk without having to deal with paper forms. The kiosks provide citizens with easy access to job information as well as expert help. The state, in turn, benefits by minimizing office space and workforce requirements and by gaining "at the source" entry of data.

Other examples of government paperless initiatives include the following:

- DoD is in the process of making its major weapons systems acquisition process completely paperless by 2000.

- The National Aeronautics and Space Administration's (NASA) Small Business Innovation Research (SBIR) contracts program is a paperless system that manages 35 percent of NASA's new contracts. It uses encryption to protect companies' proprietary data as those companies exchange information over the Internet with NASA's field centers.

- The Internal Revenue Service (IRS) encourages the electronic filing of income tax returns, which it hopes will reach 80 percent of all such returns by 2007. The IRS has found that electronic filing reduces errors, speeds processing time, and provides better security for private information.

- The Department of the Interior's Minerals Management Service (MMS) has successfully converted one of its regional public information offices into a paperless office. By using state-of-the-art technology, such as optical imaging

and advanced software for electronic retrieval, the majority of traditional paper files have been eliminated, with more than one million pages available electronically. This innovative improvement in office automation has enabled MMS to better meet the demands of nearly 18,000 annual customer requests for public information.

- "Employeeexpress.gov" is an electronic system that enables Federal employees in some agencies to control processing their own personnel and payroll data without using paper forms. Employees can access the system 24 hours a day to change their Federal and state tax withholding status, arrange for payroll direct deposit, change addresses, and make Thrift Savings Plan open-season transactions via the Web site.

SBA officials envision many potential opportunities for the Agency to automate and make its services user-friendly and more accessible through such paperless initiatives as Web sites and electronic kiosks. For example, in the future, a small business owner may be able to access the SBA Web site and select an on-line course to learn how to keep his business competitive. Alternatively, that same small business owner may be able to browse informational resources at an Agency kiosk at a convenient location any time of day.

A Cautionary Tale

Although there are many successful paperless office initiatives, a recent experience of the Social Security Administration (SSA) provides a good example of what can go wrong when such an initiative is implemented too quickly.

In March 1997, SSA began a national test of an online, interactive version of its Personal Earnings and Benefit Estimate Statement (PEBES). The Internet-based PEBES had a number of personal authenticating elements to help prevent access to PEBES by anyone other than the subject. However, after only one month of operation, the online PEBES was suspended following much criticism that its security and privacy protection measures were inadequate.

The primary problem was that an intruder could access an individual's record by obtaining such personal authentication information as name, Social Security number, date of birth, place of birth, and mother's maiden name. SSA found that the information needed to answer these questions was relatively easy to obtain from non-SSA sources.

On the advice of experts convened in a series of national public forums, SSA decided to make the service available only to people who have a registered e-mail account, such as with an employer or an Internet service provider. SSA uses the e-mail address to send the requester an activation code that, together with the personal authenticating information, unlocks an online version of PEBES. If the request is accepted through the Internet, SSA returns the information *by mail* to an address already contained in their records, providing an additional layer of protection. The entire transaction may

eventually be accomplished online, but only after proper security and authentication procedures have been thoroughly tested.

SSA concluded that, although its security efforts were not lacking, the constantly changing nature of the new electronic environment makes a diligent system security and enforcement effort vital to any organization instituting electronic applications.

RECOMMENDATION

Recommendation 6. To ensure that obsolete work processes are not automated and that electronic initiatives are compatible inside and outside of SBA, the OIG recommends that a top-level SBA official with authority over SBA programs, such as the Chief Operating Officer, lead a central coordination group of managers, staff, and technical experts to--

- **Identify any major Agency work processes that should be eliminated or performed by outside parties.**
- **Identify processes that are candidates for electronic initiatives.**
- **Refer the electronic initiatives approved by the group to the Business Technology Investment Council for detailed policy and cost evaluation.**

COPIES OF APPENDICES A, B, AND C ARE AVAILABLE UPON REQUEST.

APPENDIX D

CONTRIBUTORS TO THIS REPORT

Phil Neel, Team Leader
Michael Gaheen, Inspector
Mark Taylor, Inspector