Archived NIST Technical Series Publication

The attached publication has been archived (withdrawn), and is provided solely for historical purposes. It may have been superseded by another publication (indicated below).

Archived Publication

Series/Number:	NIST Special Publication 800-9
Title:	Good Security Practices for Electronic Commerce, Including Electronic Data Interchange
Publication Date(s):	December 1993
Withdrawal Date:	
Withdrawal Note:	

Superseding Publication(s)

The attached publication has been **superseded by** the following publication(s):

Series/Number:	
Title:	
Author(s):	
Publication Date(s):	
URL/DOI:	

Additional Information (if applicable)

Contact:	Computer Security Division (Information Technology Lab)
Latest revision of the attached publication:	
Related information:	http://csrc.nist.gov/
Withdrawal announcement (link):	

Date updated: June 9, 2015

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

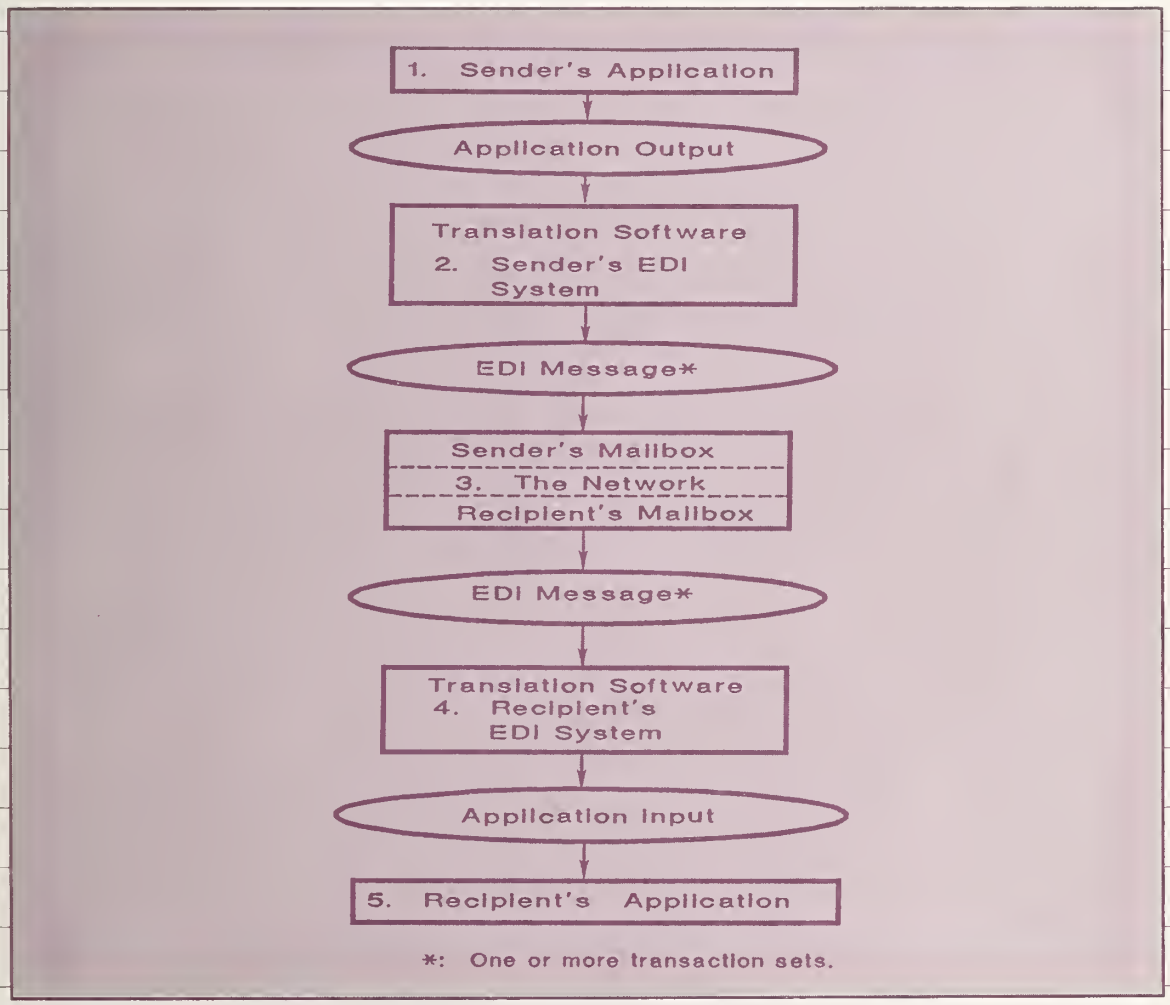
NIST Special Publication 800-9

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards and Technology

Good Security Practices for Electronic Commerce, Including Electronic Data Interchange

Roy G. Saltman, Editor

C O M P U T E R S E C U R I T Y



NIST

NIST Technical Publications

Periodical

Journal of Research of the National Institute of Standards and Technology—Reports NIST research and development in those disciplines of the physical and engineering sciences in which the Institute is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Institute's technical and scientific programs. Issued six times a year.

Nonperiodicals

Monographs—Major contributions to the technical literature on various subjects related to the Institute's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NIST, NIST annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NIST under the authority of the National Standard Data Act (Public Law 90-396). NOTE: The Journal of Physical and Chemical Reference Data (JPCRD) is published bimonthly for NIST by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements are available from ACS, 1155 Sixteenth St., NW., Washington, DC 20056.

Building Science Series—Disseminates technical information developed at the Institute on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NIST under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NIST administers this program in support of the efforts of private-sector standardizing organizations.

Consumer Information Series—Practical information, based on NIST research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

Order the **above** *NIST publications from: Superintendent of Documents, Government Printing Office, Washington, DC 20402.*

Order the **following** *NIST publications—FIPS and NISTIRs—from the National Technical Information Service, Springfield, VA 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NIST pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NIST Interagency Reports (NISTIR)—A special series of interim or final reports on work performed by NIST for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service, Springfield, VA 22161, in paper copy or microfiche form.

NIST Special Publication 800-9

Good Security Practices for Electronic Commerce, Including Electronic Data Interchange

Roy G. Saltman, Editor

C O M P U T E R S E C U R I T Y

Computer Systems Laboratory

National Institute of Standards
and Technology
Gaithersburg, MD 20899

Sponsored by:
Information Systems Security Officer
Farmers Home Administration
U.S. Department of Agriculture

December 1993

U.S. DEPARTMENT OF COMMERCE
Ronald H. Brown, Secretary

Technology Administration
Mary L. Good, Under Secretary for Technology

National Institute of Standards and Technology
Arati Prabhakar, Director

Reports on Computer Systems Technology

The National Institute of Standards and Technology (NIST) has a unique responsibility for computer systems technology within the Federal Government. NIST's Computer Systems Laboratory (CSL) develops standards and guidelines, provides technical assistance, and conducts research for computers and related telecommunications systems to achieve more effective utilization of Federal information technology resources. CSL's responsibilities include development of technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive unclassified information processed in Federal computers. CSL assists agencies in developing security plans and in improving computer security awareness training. This Special Publication 800 series reports CSL research and guidelines to Federal agencies as well as to organizations in industry, government, and academia.

National Institute of Standards and Technology Special Publication 800-9
Natl. Inst. Stand. Technol. Spec. Publ. 800-9, 66 pages (Dec. 1993)
CODEN: NSPUE2

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1993

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402–9325

GOOD SECURITY PRACTICES FOR

ELECTRONIC COMMERCE, INCLUDING

ELECTRONIC DATA INTERCHANGE

Roy G. Saltman, editor

FOREWORD

This report is an edited version of material submitted to NIST by Robert V. Jacobson of International Security Technology, Inc. of New York City, under contract number 43NANB311675. The contract was sponsored by the Information Systems Security Officer of the Farmers Home Administration, U.S. Department of Agriculture.

ABSTRACT

Electronic commerce (EC) is the use of documents in electronic form, rather than paper, for carrying out functions of business or government that require interchange of information, obligations, or monetary value between organizations. Electronic data interchange (EDI) is the computer-to-computer transmission of strictly formatted messages that represent documents; EDI is an essential component of EC. With EC, human participation in routine transaction processing is limited or non-existent. Transactions are processed and decisions are made more rapidly, leaving much less time to detect and correct errors. This report presents security procedures and techniques (which encompass internal controls and checks) that constitute good practices in the design, development, testing and operation of EC systems. Principles of risk management and definition of parameters for quantitative risk assessments are provided. The content of the trading partner agreement is discussed, and the components of EC, including the network(s) connecting the partners, are described. Some security techniques considered include audit trails, contingency planning, use of acknowledgments, electronic document management, activities of supporting networks, user access controls to systems and networks, and cryptographic techniques for authentication and confidentiality.

Key words: commerce; computer; data; electronic; interchange; internal control; security; techniques.

ACKNOWLEDGMENTS

Assistance of the following persons in the development of material for this report is gratefully acknowledged:

Mr. Michael S. Baum, Esq., President, Independent Monitoring, Cambridge, MA.
Dr. Dennis Branstad, National Institute of Standards and Technology, Gaithersburg, MD.
Mr. Robert P. Campbell, CEO, Advanced Information Management, Woodbridge, VA.
Mr. Hugh V. Davis, Director, Security and Standards Division, U.S. Customs Service, Washington, DC.
Mr. Paul Hoshall, Director, ADP/IRM Audit Division, U.S. Department of Veterans Affairs, Washington, DC.
Mr. David F. Kent, CISA, Director, Office of Information Technology and Financial Audits, U.S. Department of Transportation, Washington, DC.
Mr. F. Lynn McNulty, Associate Director for Computer Security, Computer Systems Laboratory, National Institute of Standards and Technology, Gaithersburg, MD.
Mr. Brent Melson, Information Systems Auditor, Headquarters, National Aeronautics and Space Administration, Washington, DC.
Mr. James Morgan, Manager of Security, GE Information Services, Rockville, MD.
Mr. Paul E. Moo, Electronic Commerce Consulting, Allen, TX.
Mr. Donald Mutispaugh, Defense Logistics Agency, U.S. Department of Defense, Alexandria, VA.
Mr. Edward Roback, National Institute of Standards and Technology, Gaithersburg, MD.
Mr. David Schwarz, Chief, Information Policy Branch, Environmental Protection Administration, Washington, DC.
Ms. Julie A. Smith, CISSP, Research Fellow, Logistics Management Institute, Bethesda, MD.
Mr. John L. Stelzer, Senior EDI Consultant, Sterling Software, Dublin, OH.

TABLE OF CONTENTS

TABLE OF CONTENTS
(Continued)

TABLE OF CONTENTS
(Continued)

TABLE OF FIGURES

page

1. MANAGEMENT OF SECURITY FOR ELECTRONIC COMMERCE

1.1 New Methods, New Risks

Electronic commerce (EC) is the automated conduct of business processes between and within organizations, using documents and monetary transfers that are in electronic form. EC is carried out using electronic funds transfer (EFT) for monetary interchanges and electronic data interchange (EDI) for non-monetary documents. EDI is the interchange of strictly formatted electronic documents between computers of different organizations. The strict formatting makes possible the use of computer programs to assemble electronic documents from data in computerized applications to begin an interchange and, following receipt of an interchange, to disassemble the documents and insert their data into the receiving organization's computerized applications.

The use of EC introduces new ways of carrying out business operations by eliminating paper-based commerce. The lack of hard-copy records and manual signatures raises the potential for new types of threats to the integrity of operations. Specific activities must be undertaken to assure that electronic documents are authentic, are properly authorized, are completely and accurately retained with audit trails for purposes of accountability, and remain confidential when that is necessary. In addition, operations are heavily dependent on the reliability and availability of electronic devices. It is necessary to detect and recover from error conditions, and to provide effective contingency plans in the case of system failure. It is the role of senior management to assure that the necessary practices and procedures are in place and that these requirements are met.

1.2 Functionality With Security

Senior managers have a vital role in providing for a balanced development program for EC systems that includes adequate provision for security. Authorities agree that this role is essential to successful implementation of EC systems. Senior managers must make sure that there is a proper balance between functionality and security during the design process.

Implementation of an EC system requires more care than a traditional automated business system because of four factors unique to EC:

1) Most traditional paper records are eliminated.

The electronic documents that replace paper documents are extremely important. Care must be taken to safeguard them against loss and alteration, and to ensure that any document can always be retrieved from the secure database in which it has been stored.

2) Human participation in routine transaction processing is limited or non-existent.

Human oversight in paper-based systems has provided formal and informal reasonableness testing and error detection and correction. The EC application programs and the EDI software must include comprehensive controls and checks to replace all aspects of routine human oversight while providing detection of exceptional conditions that trigger special human intervention. This report does not attempt to make a sharp distinction between "security procedures and techniques" and "internal controls and checks." Both security and control objectives are commonly served by the same measures.

3) Transactions are processed more rapidly, leaving less time to detect and correct errors.

Errors must be detected and corrected quickly, before automatic initiation of subsequent actions that will be expensive to correct.

4) Trading partners' computer systems communicate directly with one another.

Each trading partner depends heavily on the accurate and timely performance of the other partners and the data communications network that connects them. EC commonly leads to re-engineering of business systems to take advantage of the speed and efficiency inherent in EC. As a result, each trading partner must be prepared to recover quickly from system failures to avoid having an impact on operations of the other trading partners. Interrupted transactions must not be lost or incorrectly duplicated as a result of retransmission.

As long as nothing goes wrong, an EC system can function without including the security techniques described in this report. However, in the real world, accidents happen, control and procedural failures occur, and people make mistakes. Without an appropriate level of security and control, EC operation will be unreliable, and losses will be unnecessarily high. While EC systems must be protected against fraud and unauthorized disclosure of information, protection against accidents, errors, and omissions is equally important. Because of the increased processing speed of EC transactions, errors can propagate rapidly. As a result, the cost to recover from the consequences of errors and omissions tends to be greater than with traditional business systems. Consequently, prompt, accurate, and automated detection of errors and omissions is an important requirement of EC systems.

In the subsections that follow, seven topics are discussed that senior managers should consider when reviewing the plan to implement an EC system:

1) Initial considerations in planning;

2) Prudent management of the risk factors;

3) Drafting of a trading partner agreement;

4) Testing and commencement of operation;

5) The EC system contingency plan;

6) Management of electronic documents; and

7) Selection of an EDI network.

1.3 Initial Considerations in Planning for EC

An organization typically implements an EC system for one of two reasons:

1) Senior managers, together with application managers and information systems managers, determine that by eliminating traditional paper documents and their routine human processing, an EC system can yield significant savings of time and money. In this case, the organization takes the initiative, and proposes the implementation of an EC system to its trading partner(s). More and more Federal agencies and large business organizations have reached this conclusion.

2) A major customer or agency with which the organization has a business or data-interchange relationship already has an EC system, or plans to implement one. The organization is asked to do likewise. In this case, the organization is being asked either to conform to an existing EC system design or to collaborate in the design of a new EC system.

In the next two subsections, these situations are considered, and the factors that senior managers should consider when planning an EC system implementation are discussed. A senior manager, even if associated with a large organization that is taking the initiative to adopt EC, should also consider the second case. It is useful, to promote smoother implementation in the long run, to be able to see the situation from the point-of-view of the smaller organization and allow for its concerns.

Two trading partners will be assumed. However, in the general case there will be many trading partners, and references to "the trading partners" should be taken to mean all of them. Furthermore, it should be understood that, in some cases, the relationship will not involve trade in goods and services. For example, a government agency may establish an EC system to accept filings from private-sector organizations in response to its regulations. Then the "trade" is in information. For simplicity, the term "trading partners" will be used for all these relationships.

1.3.1 Initiating an EC Development Project

There are two important ingredients in a successful EC system development project: effective cooperation between trading partners in the development of the system specifications, and the adoption of a phased development plan.

When a dominant organization is initiating the development of an EC system, it may assume that it can correctly anticipate the operational needs of the prospective trading partners, and can perform the system design without consulting them. This is probably an unwise assumption, particularly regarding security issues. Many of the security techniques described in this report depend on the effective cooperation of the trading partners. Consequently, it is important to involve prospective trading partners in the development of the basic system design and in the selection of cooperative controls and security techniques and procedures.

Conceptually, the development of an EC system can be thought of as following a three-step sequence:

1) first, substitution of EDI messages for paper documents with continuation of manual processing of the EDI documents;

2) second, automated processing of the EDI messages; and

3) third, re-engineering of applications to take maximum advantage of the speed, accuracy, and standardization offered by EDI.

These steps can be described in more detail as follows:

In the first step, paper documents are translated into EDI formats and delivered electronically to the recipient trading partner. At the most primitive level, the recipient trading partner uses an EDI translation software program to convert incoming EDI messages into traditional formats and to print them. Next, the printed documents are processed as though they had been received in the mail. Similarly, outgoing documents are key-stroked from paper documents into an EDI translation software program and then transmitted to the trading partner. This is obviously a very inefficient practice, but it has the advantage of demonstrating that the "mechanical" part (the EDI part) of an EC trading partnership is functioning correctly. That is to say, the trading partners are able to exchange and translate EDI messages successfully.

In the second step, automated links are established between the existing applications and the organizations' EDI systems. Outgoing messages are generated automatically by the sender's applications, and are no longer key-stroked into the EDI system. Likewise, incoming EDI messages are translated into input files and passed to the recipient's applications automatically. The applications are

enhanced to allow for the monitoring of the EDI interface. For example, the sender's applications are modified to respond to failures of recipients to acknowledge messages on time. The recipient's applications are improved to permit the testing of the reasonableness of incoming messages more rigorously than typical edit checks and to detect duplicate messages.

In the third and final step, applications and business functions are re-engineered to take full advantage of EC. For example, advanced shipping notices sent via EDI could be used to expedite receiving dock and warehouse operations, and to initiate payment without requiring separate generation and processing of an invoice.

When an EC partnership reaches the third step, the partners get the full benefit of EC. The cost of most human processing of paper is eliminated and the attendant errors are avoided, but often there are even greater benefits from more efficient and focused operations. For example, inventories and manufacturing material stocks can be controlled more closely. The time to process orders is reduced. This evolution of existing systems to full-scale EC has repeatedly demonstrated changes that result in functional and quality control improvements. A closer and more efficient relationship is built between the trading partners.

Enthusiastic system designers may want to bypass the first two steps and go directly to a re-engineered EC system. However, converting from paper documents to EDI messages, and substituting automated processing for human oversight, are both big steps. Unexpected problems of the sort described in the remaining chapters of this report can arise. When an organization attempts to go directly from existing paper-based commerce to a phase three, re-engineered EC system, these problems are likely to emerge and cause major losses. Experience suggests that an organization without strong prior experience with EC and EDI should use a phased development. The organization should leave the existing paper-based system in place and use it to deal with the majority of the trading partners while it develops the EC system with a small subset of its trading partners.

The following guidance is proposed for prudent implementation:

1) Begin by picking a single functional area where the application programming is stable and smooth running.

2) Work with a small, but representative, subset of prospective trading partners.

3) Take each of the three development steps described above, one by one. Note that, until all of an organization's major applications have been converted to EC, only limited re-engineering is possible.

When the initial EC system development is complete, consider how to phase-in the remaining trading partners. For example, one might add trading partners in groups over time, and then expand the scope to include other applications.

It is likely that the re-engineering phase will follow paths not originally anticipated, and that the relationship with trading partners will change. These factors suggest that care should be taken to see that the system design allows for growth in size and scope, and changes in operations.

A final note: The organization that initiates an EC system should take care to avoid making unreasonable demands of its subordinate trading partners. While the dominant trading partner may have the resources and expertise to handle an EC system development project easily, this may not always be true of the subordinate partners. The dominant trading partner should take these limitations of resources and expertise into account when planning the role of the subordinate partners.

1.3.2 Joining an Existing EC System

An organization that is being asked to participate in an existing EC system may not have the opportunity to participate in the EC system design. However, the organization will have to decide how to modify its existing operations to accommodate EDI messages. The safest plan is to follow the same three steps described above, using the overall specifications already set by the other trading partner. For example, the organization may begin its participation in an EC system by setting up an EDI system that simply translates EDI messages into paper documents for manual processing. Note however, that the EC system is likely to require acknowledgment of incoming EDI messages. Therefore, it will be necessary initially to establish manual procedures to generate these acknowledgment messages. (See Section 3.2 for more about acknowledgments.)

Next, the EDI system and the applications are enhanced to pass the translated EDI messages to the applications automatically. Applications are enhanced to generate outgoing transactions automatically, including acknowledgments, for processing by the EDI system. Finally, the organization re-engineers its applications to track the operations of the dominant trading partner.

The organization should perform a risk assessment to be sure that all significant risks have been identified and will be properly addressed.

1.4 Risk Management of EC Systems

It is important to manage risk, i.e., the likelihood of loss, as the basis for wise selection of security measures. If all EC

systems were the same: i.e., the same size, transaction volume, information sensitivity, urgency, monetary activity level, and operating environment, it would be possible to define an appropriate security program and apply it to all EC systems without further consideration. This is not the case; EC systems vary in all the dimensions just enumerated. Consequently, it is not possible to define a single security program for all EC systems. EC risks can only be managed efficiently by using rational risk management. Perfect security (nothing will ever go wrong) is infinitely expensive and cannot be a rational design goal. On the other hand, inadequate security often leads to unnecessary losses.

1.4.1 Risk-Sensitive Design

Risk cannot be managed abstractly. The first step in EC system development is to develop a basic system design that accomplishes the functional requirements of the EC system. Security features need not be considered at this point. When the system design is sufficiently detailed, the risk management process can begin. There are three parts to this process:

1) Assessment of risks to determine what kinds and amounts of losses are likely to occur when the EC system becomes operational. Two loss categories are usually identified. (a) Losses caused by threats with reasonably predictable occurrence rates are sometimes referred to as "expected losses," and are expressed as average rates of loss in dollars per year. (b) If a threat has a very low rate of occurrence that is difficult to estimate, but the threat would cause a very high loss if it were to occur, the result would be referred to as a low-probability, high-consequence risk. This type of loss is often called a "single occurrence loss." Chapter Two identifies and describes the risks and vulnerabilities that are associated with typical EC systems.

2) Selection and implementation of security techniques that will (a) reduce expected losses by an amount greater than the cost to implement the security techniques, or (b) reduce the fatal losses to tolerable levels. Chapter Three suggests security techniques for consideration.

3) Periodic re-examination of risks after operational use begins to verify that security techniques continue to be effective, and to detect significant changes in the risk environment.

The initial risk assessment does not have to be highly detailed and precise. Instead, the objective should be to develop a broad understanding of inherent risks and potential security techniques to support the design effort. Thereafter, the first two steps are repeated as necessary during the design phase to refine the assessment; the selection of security techniques is optimized as the EC system design evolves.

The assessment of risks should take into account the effect of the EC technology on the effectiveness of traditional controls. Fewer people do jobs with wider scope. There is reduced routine human oversight. Separation of duties may be diminished, particularly in smaller organizations. These trends may create a situation in which one person can create a false purchase order and acknowledgment for a non-existent vendor, fake a receiving report, and trigger a fraudulent payment through electronic funds transfer.

The third step above is ongoing during the operational life of the EC system to ensure that the security program continues to meet the requirements.

1.4.2 Objectives of a Risk Assessment

Risk management has two basic objectives:

1) Optimization of the selection and implementation of security techniques, based on a rational assessment of risks. "Optimize" in this context means the implementation of security techniques that minimize the sum of future losses and security expenditures. In the case of government agencies, losses could result from compromise of confidentiality or integrity of personal or trade-secret information stored by the agency, as well as direct financial loss of material assets or funds.

2) Protection against catastrophic losses. A catastrophic loss for a private-sector firm would be a loss greater than its equity. In other words, if the loss event occurs, however unlikely its occurrence may be, the loss will bankrupt the firm. While the concept of bankruptcy does not apply in the same way to government agencies, such agencies have a responsibility to the taxpayers to mitigate exposures to material losses.

To meet these two risk management objectives, it is useful to evaluate in monetary terms the risks to which an EDI system is exposed. This enables one to measure the utility of proposed security techniques and to identify potentially catastrophic risks. An assessment of risks in monetary terms uses three kinds of input data:

1) The rate of occurrence of the threats to the EC system.

2) The loss potential associated with each of the functions performed by the EC system and each of the assets controlled by the EC system. Loss potential is the worst-case loss of an asset or function.

3) The vulnerability of the functions performed and organizational assets to each of the threats. Vulnerability is expressed as a "vulnerability factor," which is the ratio of actual loss to loss potential, and ranges from zero to one. Note that a vulnerability by itself is not significant. Even though an asset may be

vulnerable to a threat, the vulnerability is not significant unless the threat is expected to occur. Thus, a vulnerability assessment may yield useful insights about the state of existing security, but it is NOT a risk assessment.

In the real world, the details of threats, vulnerabilities, functions performed, and assets can be quite complex. Consequently, a key part of the risk assessment process is the construction of a model of the EC system that aggregates these elements into manageable groups. Initially, a model can be fairly simple. Then, as the assessment identifies the critical threats, functions, and assets, more detail can be added. This approach ensures that the analysis effort is concentrated on the key issues.

1.4.3 Quantitative Risk Assessments (QRAs)

The cost of security techniques is measured in monetary terms. Therefore, one must also measure the benefit of security techniques (the expected reduction in future losses) in monetary terms to compare cost and benefit. This is the basic reason for performing a QRA. Installing a security technique is not prudent unless its benefit outweighs its cost. The benefit of a security technique is the effect it will have on future losses. A QRA generates an estimate of the monetary losses that will occur in the future based on quantitative estimates of the threat occurrence rates, asset and function loss potentials, and vulnerabilities defined by the model of the system. QRAs are expressed in two ways:

1) Annualized Loss Expectancy (ALE). ALE is the estimated loss expressed in monetary terms at an annual rate, for example, dollars per year. The ALE for a given threat with respect to a given function or asset is equal to the product of the estimates of occurrence rate, loss potential, and vulnerability factor. If the threat's occurrence rate is less than once per year, the ALE must be understood to represent the relative significance of a threat compared with other threats. For example, imagine that the occurrence rate of a threat is estimated to be once in ten years, and its ALE is estimated to be $1,000 per year. This does not mean that the threat will cause a $1,000 loss in each of the next 10 years; it is likely to cause a $10,000 loss in one of the next 10 years, but the specific year of occurrence cannot be determined.

However, if one estimates ALEs for two threats as $1,000 per year and $100,000 per year respectively, all other things being equal, the second threat is clearly far more significant than the first one. Thus, ALE is a useful tool for ranking risks, even though confidence in ALE estimates tends to decrease as occurrence rate decreases. In other words, it is difficult to make credible estimates of occurrence rate for relative rare threats. Nonetheless, even when quantitative estimates are relatively uncertain, they may, in some cases, provide more risk management guidance than purely qualitative estimates of risk.

2) Single-Occurrence Loss (SOL). SOL is the loss expected to result from a single occurrence of a threat. It is determined for a given threat by first calculating the product of the loss potential and vulnerability factor for each function and asset with respect to the threat being analyzed. Then, the products are summed to generate the SOL for the threat. Since the SOL does not depend on an estimate of the threat's occurrence rate, it is particularly useful for evaluating rare but damaging threats. If a threat's SOL estimate is unacceptably high, it is prudent risk management to take security actions to reduce the SOL to an acceptable level.

In short, ALE is useful for addressing relatively frequent threats, and SOL is used to evaluate rare threats.

QRAs are used in three ways:

1) For selection of cost-effective security techniques. To undertake this selection, a "baseline" EC system is defined. A "baseline" EC system has just those features required to function correctly as long as no errors or failures occur. By comparing the ALE of a "baseline" EC system with the ALE of the same EC system assuming the presence of one or more proposed security techniques, one can estimate the payback of the proposed techniques. Obviously, the greater the ratio of the payback (reduction in ALE) to the cost of a security technique, the more valuable it will be.

2) For treatment of high SOLs. The SOL estimate of a threat can be used to identify the potentially fatal threats as mentioned above. While the SOL estimate cannot be used to cost-justify security measures, one can determine what needs to be done to reduce the SOL to an acceptable level. Management judgment is required to make the most effective decisions.

3) To prioritize functions and assets. An ALE can be used to prioritize functions and assets relative to one another, and to rank threats relative to one another. This information is useful when making plans for asset protection, disaster recovery, and business resumption planning.

1.4.4 Conduct of a QRA

The preceding sections have provided the basis for carrying out a QRA, but have not been highly explicit in how it might be done. Other sections of this report present additional information that may assist in this regard. For example, Section 2.3 identifies seven specific basic objectives for the security of EDI transaction sets. In the conduct of a QRA, an analyst may wish to review each of these objectives in light of the activities of the system under study, and specify the losses that would occur if the system failed in achieving any of them.

Losses may be more difficult to quantify for some security objectives than for others. For example, failure to receive goods that have been paid for (possibly due to a failure in sender authentication) may generate a clearly quantifiable loss. Even if the goods are received later, correcting the situation that caused the initial difficulty may generate an extra cost. However, loss due to compromise of confidentiality could be less clear if the organization is a government agency and the disclosure concerned personal data relating to members of the general public. The loss to the organization, which determines the selection of security measures, is distinct from the loss to the individuals. The quantitative loss to the latter could be changes in the individuals' ability to obtain future employment or advantageous business relationships. The loss to the organization might be costs of disruptive investigations, a required re-alignment of security plans and personnel, and costs compensating for the difficulty in collecting similar data in the future due to loss of confidence by the public.

1.5 The Trading Partner Agreement

When system integrators link elements of a data processing system, they speak of the "interfaces" between the system elements, and the need for each element to conform with the applicable interface specification. In a traditional business relationship between two organizations, there is no "interface specification" as such. Instead, humans interpret incoming documents, purchase orders, requests for quotations, and the like, and "translate" them as necessary to conform to internal standards. If disputes arise, they are settled based on agreements between the parties and applicable law and regulation, such as the Uniform Commercial Code, or if one of the parties is a Federal Government agency, Federal procurement regulations. These laws and regulations form an implicit "interface specification."

An essential feature of EC is the reduction or elimination of human participation in the routine processing of transactions, and the substitution of automated processing. As a result, it is essential to define precisely the details of all EC transactions. For example, the part of an EC system that composes an EDI message must use exactly the same message format as the part of the other partner's EC system that receives the message. This means that the trading partners must agree on the standards to be used and the specific details of the implementation.

Trading partner agreements (TPAs) are an important part of EC systems. They serve as the "interface specification" between trading partners and provide specific details of the legal agreements that define how the electronic commerce is to be conducted. Qualified legal advice is required when a TPA is drafted. However, the TPA must be more than a legal agreement between two organizations that interchange data. Since the TPA defines how the automated systems

will replace human inspection and interpretation of individual transactions, it must be complete and precise. The subsections that follow discuss the functions of the TPA in more detail.

1.5.1 Defining X12 Transaction Sets and EDIFACT Messages

The TPA must specify the specific transactions that the EC system is going to process, and the responsibilities of each of the partners for processing transactions. The turn-around time for responding to each EDI message should be specified. The TPA might define how frequently trading partners are required to download messages from network mailboxes. Finally, the TPA must specify what constitutes "receipt" and "acceptance" of a message by the recipient.

Of course, the TPA must include a complete and detailed specification for the format of the EDI message associated with each transaction. Currently, TPAs written in the United States commonly define message formats by reference to the EDI standards adopted by Accredited Standards Committee (ASC) X12. The X12 Committee was chartered in 1979 by the American National Standards Institute (ANSI). FIPS PUB 161-1, Electronic Data Interchange, published by the National Institute of Standards and Technology (NIST) in 1991 and updated in 1993, "adopts, with specific conditions, the families of standards known as X12 and EDIFACT," and requires the use of X12 transaction sets or EDIFACT messages if they meet "the data requirements" of an agency implementing an EC system.

The X12 Committee uses the term "transaction set" to apply to a message devised under its original syntax, data segment directory, and data element dictionary. However, the X12 Committee has voted to adopt the EDIFACT syntax by 1997. EDIFACT, an acronym for Electronic Data Interchange For Administration, Commerce, and Transport, is a family of international standards developed by the United Nations Economic Commission for Europe- Working Party (Four) on Facilitation of International Trade Procedures (UN/ECE/WP.4). The EDIFACT standards define "messages" that can be designed to be functionally equivalent to X12 transaction sets.

It may be convenient to include transaction set information in an Appendix to the TPA, and to include X12 or EDIFACT standards by reference. Note that, in general, versions and releases of these standards are not necessarily upward or downward compatible. If an existing transaction set standard does not exist, the trading partners should conform to the basic conventions used by the X12 Committee when developing their own transaction sets. FIPS PUB 161-1 states that agencies "should use current X12 and/or EDIFACT standards to the extent possible" when working with subject matter not yet considered for EDI standardization, and "shall explicitly submit their requirements for X12 and EDIFACT standards" when EDI standards do not meet agency requirements.

1.5.2 Avoiding and Resolving Disputes

Since system failures, errors, and omissions are going to occur, the TPA should attempt to anticipate each of them, and assign responsibility for their resolution. One approach to drafting the TPA is to consider the operation of the proposed EC system, and to construct a list of all the possible disputes that might arise. The results of the risk analysis will be of help here. Then, the methods of resolution of each dispute should be considered. In the best case, it will be possible to set forth in advance a sequence of steps that will lead to dispute resolution. This analysis may also suggest ways to revise or enhance the EC system controls and security measures to reduce the likelihood that a given dispute will arise, or that it cannot be resolved easily.

Coordination between the trading partners is important for success. For example, acknowledgment of messages is an important control and security technique, and is discussed in Chapter Three. However, it is essential that the trading partners agree on the details of the acknowledgment. Inadequate coordination may result in unrecognized differences in interpretation of such items as operating modes, meanings of transaction sets or messages, responsibility for exception detection, and terms of sale.

As a rule, detection of errors and omissions is much less costly than prevention. For example, recipient acknowledgment of a message can include validation information so that message alterations can be detected easily. The sender's application that processes the acknowledgment can use the validation information in the acknowledgment to verify that transaction sets were received unmodified. This kind of control is relatively simple to implement, but careful coordination between the trading partners is required to make it effective.

1.5.3 Contingency Plans and Disaster Recovery

Recovery from service interruptions, loss of data files, and destruction of system elements is another area where close coordination is required. The flow of transactions can be interrupted by a failure of any one of the five EC system elements defined in Section 2.5. The trading partners must agree on how to handle the interruptions since the actions taken will depend on which element has failed, and the estimated time required to restore service.

Each trading partner must be assured that the other partner can meet agreed-to timeliness goals. A requirement for regular disaster recovery testing should be a part of the TPA for this reason.

1.5.4 Protection of Confidential Data

One objective of the EC system risk analysis should be to identify proprietary, personal, confidential, or classified information that

must be protected against unauthorized disclosure. These data should be identified in the TPA, and the obligations of the partners to protect the data should be defined. Finally, the TPA should specify how long each copy of proprietary, personal, confidential and classified data are to be retained. See Section 1.9 for more about data retention.

1.5.5 Message Authentication and Digital Signatures

Depending on the character of the commerce being conducted, message authentication and digital signatures may be desirable or required by law or regulation. Message authentication is the process whereby the recipient of a transaction set can determine that the transaction set has not been modified during transmission. Digital signatures are elements added to a transaction set or message that are typically used as the equivalent of written signatures on paper documents. Digital signatures enable recipients to authenticate the identity of the individual originators of transaction sets. If these features are required, the TPA must identify which transaction sets are to have the features, how the features are to be implemented, and how failures to authenticate transaction sets and signatures are to be resolved. This topic is discussed in more detail in Sections 3.3.5 and 3.3.6.

1.5.6 A Model TPA

A model TPA has been developed by the American Bar Association, and it can be useful in the initial stage of preparing an agreement. The model agreement stresses the contractual issues; it could serve as a useful point of departure for the drafting of an applicable TPA. For a Federal agency, the model TPA should be considered in connection with the requirements of Federal Acquisition Regulations.

1.6 The EC System Test Plan

Experience shows that careful and complete testing is essential to successful implementation of EC systems.

Case Study: A sender's EDI system was designed to use the output it received from an application each day to overwrite a permanent file that served as input to the EDI translation program. The EDI system was never tested for the case when the output from the application was of zero size. Later, during operational use, it was discovered that when the output was zero, the permanent file was not overwritten. As a result, the prior day's transactions were processed again, resulting in the dispatch of duplicate transaction sets. It was necessary for the recipient to "undo" the duplicate sets manually.

Examples like this underscore the point that EC system failures are

particularly troublesome because they usually involve the other trading partner. Recovery and corrective actions are more difficult when more than one organization is involved. It is essential to verify that all interfaces will work correctly regardless of input errors and omissions.

The following are suggestions for the construction of a test plan:

1) Begin by testing the interface between the applications and the EDI system. Test all transactions at all boundary conditions, and verify correct translation. Simulate all possible error conditions and verify correct response of the applications and the EDI system.

2) Simulate trading partner input from the network to the EDI system; verify correct translation and delivery to the recipient applications.

3) When all sender and recipient processing have been completely tested, conduct tests to simulate EDI traffic in both directions at the planned activity levels. Verify correct handling of potential overload conditions such as month-end, quarter-end, and year-end, when traffic levels may be high and timeliness is critical.

4) When both trading partners have completed the above tests in-house, test the EC system operation between trading partners using test transactions and the network. Note: it is essential to be able to generate test transaction sets during initial acceptance testing, and later when adding enhancements to the EC system. The recipient of test transaction sets should always be able to distinguish them from live transaction sets.

5) Using test messages, simulate emergency conditions to verify that the contingency recovery plan works as expected and that trading partners understand their roles. For example, simulate network or EDI system failures that occur during processing of a stream of transaction sets to verify that interrupted transaction sets can be identified and recovered. (Connections could be unplugged or switches temporarily reset to undertake such a simulation.)

Independent testers should design the tests based on the system specifications, with the goal of demonstrating that the system works as intended regardless of input errors, system errors, and breakdowns. The designers of an EC system should not design, conduct, or evaluate the tests of the system because they will have a natural tendency to prove that the system works as designed using normal inputs and under normal conditions. Test planning is also discussed in Section 3.11.

1.7 Commencement of Operation

As noted in Section 1.3, it is prudent to use a phased implementation to minimize the impact of the inevitable problems. Specifically, the plan should keep the prior traditional system in operation during development, to provide a fallback option. If the organization that initiated the implementation of the EC system has many smaller trading partners, a small subset of them should be selected for readiness testing, and then operational use. After a reasonable trial period, additional trading partners can be converted to the EC system.

Here is a checklist of points to consider when planning the implementation:

1) Use stepwise testing to confirm that the hardware, software, and procedures work correctly by conducting tests in the following order:
(a) application to EDI system;
(b) EDI system to application;
(c) EDI system to EDI System;
(d) application to application.

2) When the system design has stabilized, conduct a training program for operating personnel of both trading partners.

3) Begin operation on a limited scale as discussed above; broaden the scope as confidence grows.

1.8 The EC System Contingency Plan

Just as with conventional data processing systems, it is essential to construct and maintain a contingency plan. The plan should enable the trading partners to respond to, and recover from, system failures ranging from the failure of individual system elements to catastrophic events that destroy buildings and their contents. Contingency planning for an EC system is complicated by two factors: (a) the dependency of trading partners on electronic interchanges, and (b) the reduction in human oversight.

The TPA should describe how partner contingency plans will provide for factors like these:

1) How and under what circumstances a trading partner notifies other partners of service interruptions.

2) What modifications, if any, will be made to timeliness requirements if there is a service interruption.

3) The extent to which one partner will assist another partner to recover data lost in a disaster, and the terms under

which the assistance is provided.

The TPA should also define how and when trading partners will conduct joint contingency tests. See Section 3.9 for more about this.

1.9 Management of Electronic Documents

It is important to be sure that documents that are in electronic form are available to comply with legal retention and disaster recovery requirements, and to satisfy auditor needs. However, EC systems can make it more difficult for a data owner to control access to data held by others. To ensure the ability to recover from failures promptly, EC systems typically store copies of a given electronic document in more than one place. For example, the record of a confidential price quotation might exist in a sender's application on-line and back-up files, the sender's EDI system back-up files, the value-added network's (VAN's) back-up files, the recipient's EDI system back-up files, and one or more of the recipient's application files. The TPA should address the questions of data ownership, and how long nonowners are permitted to retain data to protect the property rights of trading partners. See Section 3.7 for more about electronic document management.

1.10 Selecting a Network

Trading partners need to be connected to a data communications network that can transmit their EDI transaction sets. Selection of a network is important because it will influence the performance of the trading partnership in two quite different ways:

1) The technical characteristics of the network, its traffic handling capacity, its data protection and data integrity, and its reliability/availability must meet the needs of trading partners.

2) VAN status-reporting services can be used to support security and control objectives.

Network considerations are discussed in Sections 2.10, 2.11, and 3.5. It is important to identify the network arrangement that will provide the best overall cost/performance for the trading partners including security and control considerations. If a third party network is used, the network agreement that the trading partners sign should include provisions such as the following to meet the requirements of the trading partners:

1) Physical and logical controls over access to trading partner messages by both network personnel and outsiders.

2) Provisions for administration by the network of trading

partner identifications (IDs) and passwords used to control access to the network.

3) Performance warranties of network availability, accuracy of message transmission, and message delivery time.

4) Retention of messages to permit recovery from disasters.

5) Retention of logs to permit subsequent audit of activity.

The specific details of the network usage should be fully defined in an appendix to the TPA.

2. IDENTIFICATION OF ELECTRONIC COMMERCE SYSTEM RISKS

2.1 Introduction

This chapter discusses operational aspects of EC and EDI that lead to the unique risks of EC systems. If the initial risk assessment of an EC system is inadequate, some risks may be ignored or understated, resulting in inadequate security measures. As a result, excessive protection may be provided against other risks, resulting in wasted resources. The information in this chapter can be used to structure the risk analysis to be sure that all potential risks are evaluated. Section 2.16 discusses general risks that are not specific to EC systems, but that should be included in the risk analysis.

2.2 Basic EC and EDI Operations

The objective of EC is to minimize or eliminate paper documents and routine human participation in processing, to reduce costs and improve performance. For example, in a traditional paper-based trading process, personnel at government agency ABC compose and print a purchase order and cause funds to be reserved in the agency's financial system. The purchase order is reviewed and signed by a contracting officer, and mailed to company XYZ. At company XYZ, a salesman verifies price, quantity, and shipping date. An order entry clerk uses a computer workstation to enter the purchase order information into the XYZ order entry system.

Case Study: Experience shows that for typical business systems such as the example above, about 70% of the mismatches between documents, (for example, the price shown on a purchase order and on the subsequent invoice), are caused by keystroke errors when data are entered from paper documents. The direct cost to correct these relatively simply errors ranges from about $7.50 to $25.00 each. Consequential costs are likely to be much higher if the errors are not detected promptly. EC systems have the potential to eliminate most of these errors.

When ABC and XYZ agree to use EC, the purchase order document and most of the human processing are eliminated. A contracting officer at agency ABC releases the purchase order from a computer workstation. Under some circumstances, a routine purchase order might be generated automatically in response to a message from an inventory control system, when the product needed is obtainable as a delivery order under an existing contract. The purchasing system then transmits the purchase order information to ABC's EDI computer system while automatically informing the agency's financial system. The EDI system translates the information into a standard EDI transaction set, and passes it to a communications network used by ABC and XYZ.

The communication network puts the transaction set in XYZ's "mailbox." Later XYZ's EDI computer retrieves the transaction set from its "mailbox." The EDI computer then translates the transaction set from the EDI standard format into a data file record that is compatible with XYZ's order entry system, and passes the file to the order entry system. The order entry system automatically performs the various checks. If there is an exception condition, for example an invalid part number, human intervention is triggered. Otherwise, the order is processed automatically. For example, the order entry system might send an Advance Shipping Notice transaction set back to ABC with full details of how the order is being processed.

2.3 Defining Threat, Risk and Security

A threat can be thought of as a potential event that has some non-zero probability of occurrence, and which causes a loss when it occurs. Risk, defined in Section 1.4 as the likelihood of loss, may be considered with respect to the occurrence of a particular threat. The term security is used in its broadest sense in this report. A security technique is any action taken to reduce the risk associated with a particular threat occurrence. A security technique may be an application of a policy or procedure, use of a hardware device, or implementation of a software feature.

The boundary between operational and security issues cannot be sharply defined, and the reader may feel that a "security technique" described here is simply "good system design practice." Perhaps the best distinction is between techniques required simply to make the EC system work correctly when all the system elements perform exactly as expected, and the techniques required for acceptable real-world operation when, inevitably, performance is not flawless.

Indeed, an EC system can be implemented without applying the "good security practices" described in this report. If testing is inadequate, the system may appear to function satisfactorily. If nothing can go wrong at any time, good security practices are not required. However, both analysis and experience suggest that the threats described in this report may occur. These occurrences will have a significant negative impact on EC systems unless good security practices have been implemented.

Note that the mere existence of a threat is not, of itself, sufficient reason to install a security technique. The need for a technique depends on the magnitude of the loss it is expected to reduce or eliminate. The magnitude of the loss resulting from a threat occurrence depends on several factors:

1) the anticipated rate of occurrence of the threat;

2) whether the threat occurrence is accidental or deliberate; there may be a greater loss if an EDI message is maliciously and carefully altered than if it is accidentally and randomly changed;

3) the type of transaction: information versus action;

4) the volume of transactions per day exposed to the threat;

5) the urgency of the transactions;

6) the monetary value of the transactions; and

7) the dependence of other processing systems on the system being considered.

It is not a sound management practice to expend resources protecting against threats that will not have a significant loss impact, i.e., risk. Since the relative importance of threats and vulnerabilities is not always obvious, it is important to conduct an adequately detailed risk analysis as described in Section 1.4 to ensure that security resources are allocated wisely.

Some EC risks are inherent in the basic concept of EC. Others are specific to the five individual elements of EC systems as defined in Section 2.5. The following are basic objectives for the security of EDI transaction sets:

1) Content Integrity. Content cannot (easily) be altered, or detection of alteration is assured.

2) Sequence Integrity. Detection of missing, duplicated, or out-of-sequence transaction sets is assured.

3) Content Confidentiality. Depending on the sensitivity of the contents, the probability of an unauthorized disclosure is acceptably low.

4) Sender Authentication. The recipient can verify the originator. Note: The term "sender" is used here to mean an organization, for example a government agency, or a corporation. However, in some instances there may be an additional requirement to authenticate the individual by name who "signed" (authorized the dispatch of) a transaction set.

5) Recipient Authentication. The sender can verify that the intended recipient received the document.

6) Timely Delivery. EC system reliability ensures that transmission of transaction sets from sender to recipient meets timeliness goals.

7) Exclusive Delivery. A transaction set should only be

delivered to the intended recipient.

Note the difference between using either prevention or detection to achieve these objectives. In many cases, detection is significantly cheaper than prevention, but it requires a recovery action when an error or exception condition is detected. The cost of recovery should be added to the direct cost of the detection method to determine the total cost. Preventative measures should only be adopted to achieve a security objective when it can be shown that the risk reduction warrants the extra cost. It should be noted that it is difficult to detect unauthorized disclosure of information. Prevention using cryptography may be less costly and more reliable than detection.

Much of EC security focuses on the need to find automated substitutes for the human oversight that characterizes traditional paper-based business transactions. There are four generally applicable EC system good security practices that support this objective:

1) Automated Acknowledgment. As transaction sets pass from the sender's application to the recipient's application, acknowledgments are passed back and processed automatically. Each system element in the transmission path maintains a log of the transaction sets it is processing. Each log record includes a note of the time by which acknowledgment must be received. A negative acknowledgment (the transaction set is invalid and was rejected) or failure to acknowledge within the specified time limit triggers an exception condition requiring appropriate resolution, possibly involving human intervention. See Section 3.2 for a detailed discussion of this topic.

2) Maintenance of Audit Trails and Archival Records, and Electronic Document Management. Since the elimination of paper records is an essential characteristic of EC systems, care must be taken in the design and operation of EC systems to ensure that the electronic documents that the systems create and maintain will be accepted by law courts and auditors as the equal of equivalent paper documents that are "records kept in the ordinary course of business."

3) Careful Definition of All Aspects of the Transactions. The EDI transaction set standards developed by the X12 Committee serve to define the technical structure of the EDI messages passed between trading partners. These standards should be used in EC system design to the extent possible. Well-drafted individual trading partner agreements (TPAs) define in detail how each transaction set is to be processed, and the liability of each partner regarding all abnormalities.

4) Authentication. Where warranted by the level of risk, security techniques are employed to give trading partners confidence that individual transactions are authentic. This may include

the use of authentication codes and digital signatures with transaction sets. See Sections 3.3.5 and 3.3.6 for more about this.

In the sections that follow, specific implementations of these recommended practices are discussed.

2.4 General EC System Security Requirements

1) Coordination between partners must be complete.

Coordination between trading partners must be complete to protect against unrecognized differences in interpretation of operating modes, meanings of transaction sets, responsibility for exception detection, cryptographic key incompatibility, differences between printed information and electronic data, etc.

2) The TPA must adequately define "terms of sale" and other duties and obligations of the partners; legal liability should be adequately defined and assigned.

A traditional printed purchase order form includes terms of sale. Because of the nature of EC, the terms of sale and other duties and obligations of the trading partners are defined in advance before individual transactions take place; they are included by implicit reference in each transaction. Since EC introduces new elements into the conduct of business and reduces human review and approval of transactions, it is essential that the TPA be complete and unambiguous about terms and conditions that apply to transaction sets. Similarly, the TPA must adequately define and assign responsibilities for unsatisfactory operating results causing unexpected liability.

3) EC system records must be adequate to satisfy legal requirements for their trustworthiness.

It is generally recognized by courts that records "maintained in the ordinary course of business" may be admitted as evidence. Since many if not all the records of EC transactions are stored electronically rather than on paper, it is important to be sure that the way in which such records are structured, created, recorded and stored will allow them to be accepted as trustworthy.

4) Implementation should be complete and effective to avoid conflicts between electronic documents and printed material.

Care must be taken with the details of the implementation to anticipate and resolve possible ambiguity in the interpretation of EC transactions. The TPA and the methods used to create and maintain computerized records of prices, part numbers and descriptions, and the like should completely replace paper records similar factors. Otherwise, there is a risk that a trading partner will use obsolete

information from a paper document, for example, an out-of-date catalog or price list, to compose a transaction set. Ideally, information of this sort should be exchanged using EDI and incorporated automatically into the applications using the information.

5) EC system reliability must satisfy trading partner requirements for timely processing.

The designers and users of an EC system have expectations about the reliability of the hardware and software. Hardware and software failures, and human errors may result in (a) processing delays, (b) lost transaction sets, logs, and data files, and (c) unauthorized disclosure of information. The reliability expectations should be explicitly defined; the details of the hardware and software design and implementation, and the operating procedures, should ensure that these expectations are met.

6) Audit of EC systems should be effective.

Audit of EC systems must be adequate in scope, depth, frequency and technical competence to ensure timely detection of material deficiencies. See Section 3.8 for a discussion of this topic.

7) Transaction set authentication must be commensurate with the risk of repudiation or deception.

Because paper documents and human oversight are both minimized or eliminated, there is a risk that a trading partner may claim that a transaction set was not sent or received, or that the content of a transaction set is different than understood by another partner. This is sometimes referred to as repudiation. The EC system design should include features to minimize:

(a) uncertainty about the flow of transaction sets between trading partners, and

(b) the possibility that changes (both accidental and deliberate) to a transaction set will not be detected.

The term "non-repudiation" was devised by technical experts to characterize EC systems that employ cryptographic techniques in order to assure that a trading partner could not deny transmission or reception, or deny specific message content. The term was used because of the assumption that one could not repudiate cryptographically authenticated transaction sets. In fact, a trading partner is always free to repudiate a transaction set regardless of the authentication technique used. It is more accurate to say that repudiation is discouraged with use of an authentication technique that provides evidence difficult to refute.

Ultimately, the authentication characteristics of a transaction set simply contribute to the weight of the evidence in a legal action,

but the courts decide if the repudiation of a transaction set will be upheld or overturned. Thus, we conclude that the strength of the authentication method used by an EC system should be commensurate with the risk of repudiation. Sections 3.3.5 and 3.3.6 discuss authentication techniques, and Section 3.2 describes the use of acknowledgments to support the objective of non-repudiation.

8) Only authorized accesses to EC systems must be permitted.

Unauthorized access to computer systems is a significant problem in many organizations. Such access may be obtained from inside or outside the organization, e.g., via compromise of passwords and identifications, or compromise of telephone numbers and communications equipment. Poorly protected databases and access points for maintenance and computer system management personnel are vulnerabilities that can be exploited. Additional information on protective techniques may be found in NBS SP 500-137, Security for Dial-Up Lines; NIST SP 500-171, Computer User's Guide to the Protection of Information Resources; FIPS PUB 112, Standard on Password Usage; and FIPS PUB 181, Automated Password Generator.

Unauthorized accesses may be for the purposes of sabotage or for obtaining sensitive data. Data in trading partners' systems may have value to parties unauthorized to receive them. These data are vulnerable while in the sender's or recipient's applications and while being interchanged through EDI. Types of data subject to compromise may include personal data such as salaries and records of health conditions, and trade secrets such as bids in response to requests for quotes and plans for new business initiatives.

9) Passive wiretapping should be prevented for a system at risk.

There is no infallible way to detect passive wiretaps. Consequently, prevention is a more reliable safeguard than detection, but the cost of prevention is justified only if there is a significant risk. The risk of interception depends on two factors: (a) the character of the contents of a transaction set as a motivation to intercept it, and (b) the extent to which the transmission path is vulnerable to wiretapping. In other words, the value to an intruder of the information obtained from a wiretap must be perceived by the intruder to be significantly higher than the cost (including the risk and consequences of being caught in the act) of installing and operating the wiretap. Vulnerability alone does not automatically create a high risk and justify the cost of prevention.

Practically speaking, it is very difficult to identify a particular organization's transmissions in the stream of transmissions in a multi-user network unless one has full access to network facilities. Consequently, wiretaps are most likely to be placed on or near a trading partner's premises where circuits can be accessed and identified. If the nature of the information being transmitted

suggests that wiretapping is a serious threat, then care should be taken to control access to telephone closets and other locations where circuits are accessible. Encryption of messages raises the cost of interception sharply.

10) Techniques should be used against active wiretapping when needed.

The term "active wiretapping" is used here to refer to the act of intercepting a transaction set, making changes to the transaction set intended to benefit the intruder, and then inserting the transaction set back into the data stream. Similar to passive wiretaps, the risk of active wiretaps depends on the extent to which a potential intruder perceives that the benefit of making a modification outweighs the cost.

Note that the cost to modify a transaction set is significantly higher than mere interception. Deliberate modification implies that specific transaction sets are being targeted. In most cases it would be quite difficult technically to locate a specific transaction set, intercept it, modify it, and then insert it back into the data stream without causing an error condition or otherwise having the modification activity detected.

One location at which intentional modification could occur is at a VAN used as part of the process transmitting the transaction set to trading partners. VAN users should assure themselves that VAN security procedures and contractual arrangements with the VAN significantly lower this possibility.

Software analyses on received data that checks for reasonableness of values and compares values in the same fields of different messages from the same trading partner may be used as aids in the detection of alterations, both deliberate and accidental. Techniques for prevention, in addition to detection, may be employed if active wiretapping is a serious threat and satisfactory methods of detection cannot be devised. Cryptographic techniques for authentication and confidentiality also protect against transaction set modification.

11) Protective measures should be implemented against system sabotage and natural disasters that could disrupt operations.

Once trading partners have abandoned the traditional processing systems, their strong dependence on EC makes the system an attractive sabotage target. Similarly, a natural disaster such as a flood, fire, or power or telephone outage could disrupt operations significantly. It is important to provide effective physical protection for EC system facilities, and to maintain effective contingency plans.

2.5 Risks Specific to the Five Elements of an EC System

EC is characterized by the automated transmission of transaction sets between the computerized business applications of trading partners using five basic elements. Some risks apply to specific elements of an EC system. The five elements are as follows:

1) The Sender's Application. The computer application that generates EDI documents, for example, a procurement system that generates purchase orders.

2) The Sender's EDI System. The computer and communications system that receives a document from a sender application, translates it into a standardized EDI format, and passes it to the network.

3) The Network. The communications facility that passes EDI transaction sets from the sender's EDI system to the recipient's EDI system.

4) The Recipient's EDI System. The computer and communications system that receives an EDI transaction set from the network, translates it into a compatible format, and passes it to a recipient computer application.

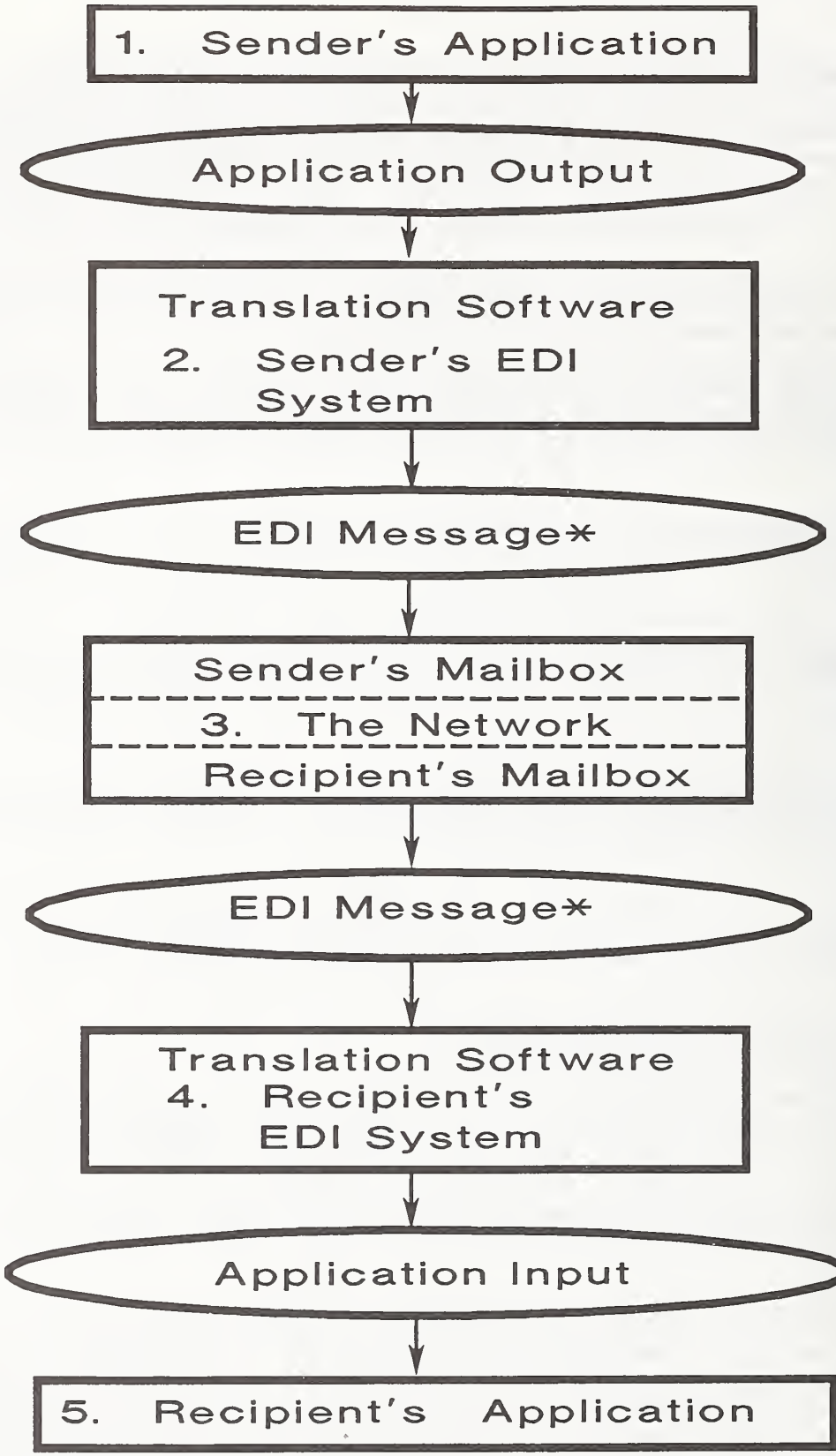
5) The Recipient's Application. A computer application that receives and processes the information in an EDI transaction set, for example, an order entry system.

Figure 1, p. 28, shows the relationship among these five elements graphically. Each of these elements and the associated risks are described in more detail in the subsections that follow.

2.6 The Sender's Application

A typical sender's application accepts inputs, maintains a database, and generates output. In a paper-based system, some of the output is traditional business documents. These documents are transmitted to trading partners by a number of different methods such as mail, courier services, fax, and telex. In EC, the sender's application sends output to the sender's EDI system for processing.

For example, a sender's procurement system maintains a list of approved vendors, accepts purchase order information, initiates purchase orders, maintains a database of outstanding purchase orders, and generates purchase order transactions that it passes to the sender's EDI system. Each transaction in the output file must contain all the information required by the EDI system to compose the EDI transaction set.



*: One or more transaction sets.

Figure 1. The Five Elements of an EC System.

Fully developed EC systems will interconnect applications to eliminate routine human intervention where possible. For example, an inventory control system will detect the need to replenish the stock of a purchased item and send a "requisition" to the purchasing system. The purchasing system will consult its database and identify vendors of the item, and pricing information. It may generate a purchase order transaction automatically if it can associate the needed item with an open contract from which deliveries may be obtained. Otherwise, it could inform an inventory specialist of the need to issue a request for quotes. (For certain well-defined stock items, the issuance of a request for quotes could be done automatically as well). Ideally, the purchasing system receives pricing and part number update data from vendors as EDI transaction sets, and updates its database automatically.

2.7 Potential Risks of the Sender's Application

Hardware and software failures of the sender's application cause the following risks:

1) The content of a transaction is incorrect.

2) A transaction is not initiated as expected, and is not passed to the EDI system.

3) A transaction is misaddressed, and does not go to the intended recipient.

4) A duplicate transaction is generated and sent to the recipient.

5) A failure to reconcile transactions with the EDI system's list of transaction sets processed is not detected.

2.8 The Sender's EDI System

The sender's EDI system receives transactions from the sender's application, usually in the form of flat files of transaction records. While the details of the implementation may vary, the typical sender's EDI system has two major computerized parts: a translation program, and a network interface.

The function of the translator is to convert the output from the sender's application into standard EDI message formats called transaction sets. Each transaction set defines the precise arrangement of the contents of an EDI message. For example, the X12 Committee has defined a number of transaction set standards. Each standard is identified by a number and name. Some typical X12 transactions sets are: 810 Invoice; 820 Payment Order; 840 Request for Quotation; and 997 Functional Acknowledgment. Each transaction

set is made up of data segments, each of which consists of one or more data elements. The structure of the X12 standards allow data segments and data elements to be used in more than one transaction set. The Data Interchange Standards Association (DISA) Publications Catalog, issued annually, includes an excellent summary of these concepts, and lists the transaction set standards. DISA serves as the secretariat for the X12 Committee.

The translator creates a transaction set, for example an 850 Purchase Order, by converting transaction data fields in the application's flat file into the required transaction set data elements and data segments. The translator follows mapping information supplied to it by its designers. The X12 standards allow two or more transaction sets of the same type going to the same recipient to be assembled into what is called a functional group. Any number of functional groups going to the same recipient can be assembled into a single message using within what is called the interchange envelope. The translator includes in the interchange envelope the information needed to identify the recipient to the network.

The network interface passes the transaction sets to the network, and maintains appropriate transaction logs to ensure that all transaction sets are delivered to the designated recipient.

2.9 Potential Risks of the Sender's EDI System

The possibility of hardware and software failures of the sender's EDI system, and misfeasance or malfeasance of EDI system personnel result in the following risks:

1) A error in translating a transaction into EDI format (incorrect or incomplete information) is not detected and corrected. Thus, an invalid transaction set is sent to the network.

2) A valid transaction set is corrupted before being passed to the network.

3) An incorrect recipient identification is added to a valid transaction set before it is passed to the network.

4) A valid transaction set is created from a sender's application transaction, but is not queued for transmission.

5) A valid transaction set is transmitted more than once.

6) The expected acknowledgment of a transaction set is not received within the stipulated time, but an exception condition is not generated.

2.10 The Network

The term "network" is used here to refer to the facilities used to connect the sender's and recipient's EDI systems. There are four basic kinds of network configurations used by trading partners:

1) Point-to-point. Two trading partners may communicate directly with one another through a dial-up common carrier network or a dedicated circuit. The sender's EDI system communicates directly with the recipient's EDI system. The "network" does not have a storage capability, and does not provide any message status information.

2) Use of a Single Value-Added Network (VAN). The trading partners use a common VAN to communicate. The typical VAN simplifies communications for a sending partner who has many receiving partners. The VAN accepts messages from the sender and passes them to the recipients; the sender does not have to contact each recipient separately. Each VAN user is said to have a "mailbox." When the VAN receives a message from a sender, it reads the address on the message "envelope" (header) to identify the recipient. The VAN then moves the messages from the sender's mailbox to the recipient's mailbox. Later the recipient's EDI system connects to the VAN, discovers the message and downloads it. This method of operation is often called "store-and-forward."

A VAN can report to a sender when it deposits a message in a recipient's mailbox, and when the recipient removes the message from his or her mailbox. This confirms to the sender that the recipient has the message, and helps to support the authentication of both the sender and recipient.

3) Use of Two VANs. If trading partners are users of different VANs, it may be possible to arrange for a VAN-to-VAN connection. Operation is the same as described above, except that the message must first move from the sender's VAN to the recipient's VAN. VANs typically maintain gateways to other VANs as a service to their subscribers. It is desirable for the sender's VAN to be able to report complete status information back to the sender about the delivery of a message to the recipient and the recipient's retrieval. If the two VANs cannot interchange complete information, then the sender's VAN may only be able to report to the sender that the message was passed to the recipient's VAN but not to the recipient. In this latter case, knowledge of timely delivery to the correct party is not assured to the sender. Use by the VANs of the X.400 communications protocol, or the X12 Committee's X12.56 Interconnect Mailbag Control Structures, may provide the necessary support to provide the needed information.

4) Dedicated Network. The dominant trading partner provides and operates the network that the subordinate trading partners use to send and receive EDI messages.

2.11 Potential Network Risks

The possibility of network hardware and software failures, misfeasance or malfeasance of network personnel, and actions by outsiders can result in risk. As noted below, some risks do not apply to all network types.

1) A message is delivered to the wrong recipient. This risk does not apply to messages from a subordinate partner to a dominant partner on a dedicated network, or on a dedicated point-to-point network.

2) Undetected corruption of a message occurs.

3) Failure of a message to reach the recipient is not detected. (Applies primarily to use of VANs.)

4) A VAN incorrectly reports to the sender the status of message pickup by the recipient. For example, the pickup occurred significantly later than reported, or was not reported when it occurred.

5) A message is delayed in transmission significantly longer than expected. What constitutes a significant delay will depend on the character of the message. If the network is a VAN, the usage agreement should specify the expected delivery time.

6) A message is intercepted and disclosed to others without authorization. This risk applies to all network types, but a wiretap is not required on a VAN since messages typically are stored on back-up files, and VAN personnel routinely monitor traffic.

7) A message is intercepted and modified without authorization, and then transmitted on to the recipient.

2.12 The Recipient's EDI System

The recipient's EDI system performs functions similar to the sender's EDI system, but in the opposite sequence. The EDI system receives messages from the EDI network, translates the EDI transaction sets in the messages, e.g., one or more 850 Purchase Orders, into in-house formats, and passes them to the appropriate recipient's applications. The translations make use of maps to relate transaction set data elements to data fields of the transaction files passed to the applications.

The EDI system may also generate a 997 Functional Acknowledgment transaction set and transmit it to the sender. Note that the name of this transaction set is not fully descriptive. The sender can only conclude that the transaction set being acknowledged was re-

ceived intact by the recipient, but not that it was accepted by a recipient application. For example, a functional acknowledgment of a purchase order transaction set does not constitute acceptance of the purchase order. The 997 Functional Acknowledgment is the EDI equivalent of a U.S. Postal Service return receipt.

2.13 Potential Risks of the Recipient's EDI System

The possibility of hardware and software failures of the recipient's EDI system, and misfeasance or malfeasance of EDI system personnel results in the following risks:

1) An EDI message is received from the network but not otherwise processed.

2) An EDI message is received from the network but no acknowledgment is sent as expected by the network or the sender's EDI system.

3) A transaction set is acknowledged as received, but is lost internally before it is passed to the correct recipient application system.

4) Incorrect translation of a transaction set is not detected. The wrong acknowledgment is sent.

2.14 The Recipient's Application

The recipient's application receives and acts on the translated transaction sets received from the recipient's EDI system. Functionally, this is the same as receiving the data from key-stroked, paper source documents.

If one of the transactions sets is an 850 Purchase Order, for example, the order entry application validates the transaction. If it is acceptable, the application generates an acknowledgment transaction, for example, an 855 Purchase Order Acknowledgment transaction set, and sends it back to the sender. In a fully re-engineered EC system, the order entry application might also transmit input data to the warehouse, inventory control, customer credit, accounts receivable, and shipping systems to fulfill the purchase order.

2.15 Potential Risks of the Recipient's Application

Hardware and software failures of the recipient's application result in the following risks:

1) An invalid or corrupted transaction is not detected.

2) Receipt of a valid transaction set is not acknowledged by the recipient as expected by the EDI system and/or the sender.

3) Receipt of a duplicate transaction set is not detected.

4) Invalid translation of a transaction set is not detected.

5) The application does not reconcile its table of transactions processed with the EDI system's table of transactions passed to the application.

2.16 Risks Not Specific to EC Systems

EC systems typically are connected to business data processing systems that relate to other activities. Examples of such data processing systems are those for finance, accounts payable and receivable, inventory and shipping. These traditional data processing systems are exposed to general risks that are not specific to EC systems, but that could affect them. Some of these risks are:

(1) Service interruptions to general data processing systems caused by risks such as hardware and software failures, fires, floods, earthquake, sabotage, etc.

(2) Application fraud due to staff personnel entering falsified transactions or data into general data processing systems or by modifying applications or operating system programs.

(3) Unauthorized disclosure of information, by means of reports or files generated or maintained by general data processing systems to which EC systems are connected.

These risks may already have been analyzed as a part of an existing risk management program. In any event, they should be included in the risk analysis of the EC system.

3. GOOD SECURITY PRACTICES

3.1 Summary

This chapter describes good security techniques that apply during the design, test, and operational phases of EC systems implementation, and it addresses the special requirements of EC systems. These techniques include subsystem-to-subsystem acknowledgments and other techniques, especially for the application, EDI, and network subsystems. In addition, access controls, electronic document management, audit trails, contingency plans, compliance audits, and system testing are discussed.

A security technique should not be adopted simply because it is described here. It should only be included in an EC system if it is expected to have a beneficial impact on the operating cost of the EC system. That is, it should be used if the expected reduction in losses will outweigh the cost to implement the security technique, or the security technique will address an unacceptably high single-occurrence loss.

3.2 Use of Acknowledgments

Use of acknowledgments is a good security practice; it is fundamental to secure EC because it addresses several important risks:

1) duplicated transaction sets generated in error by the sender's application or EDI system, the network, or the recipient's EDI system;

2) repudiated transaction sets;

3) lost transaction sets; and

4) invalid or corrupted transaction sets.

The most important risk addressed by an acknowledgment is the duplicate transaction set. A recipient cannot detect a transaction set that the sender's application has duplicated by mistake, since (as discussed in Section 3.3.1) the two transaction sets should have different sequence numbers. The expense of subsequent corrective action may be quite high. For example, a recipient may take a high-cost action, e.g., fabricate custom-designed parts, in response to an undetected duplicate purchase order. However, a detailed acknowledgment of the inadvertently duplicated transactions should enable the sender to detect the duplication and take prompt corrective action.

Every EC message should be acknowledged with a message from the recipient's application sent back to the sender's application,

within a stipulated time defined in the TPA. The TPA should define the action to be taken by the sender if an acknowledgment is not received on time or is negative, and should define the imputed significance of acknowledgment. Note that acknowledgments are NOT acknowledged.

Acknowledgment can be used to support non-repudiation. For example, consider the vendor who asserts that a Request For Quotation (RFQ) was not received. If the TPA calls for a positive acknowledgment, the sender will have a record of the acknowledgment message from the recipient. Acknowledgment from a VAN specifying delivery to the recipient also provides evidence to refute repudiation. Assuming good system design, the sender can show how the RFQ system matched each incoming acknowledgment against the list of bidders, and how the sender followed-up promptly when acknowledgments were not received on time.

Similarly, imagine that a bidder attempts to disavow a low bid when an order is received. If the agency issuing the purchase order acknowledges all bids received before "opening" the bids, it can then show that the low bidder did not question the acknowledgment of the receipt of that bid by the agency.

Acknowledgment also supports prompt detection of data corruption and lost messages. Either the EDI systems or the network may fail in such a way that a message is lost in transit and does not reach the recipient's application. Likewise, hardware or software failures may corrupt a message or make it invalid. Because routine human oversight has been eliminated, it is important to be able to detect such failures automatically, and trigger prompt human intervention.

There are five kinds of acknowledgments. Each one is separately described below and shown graphically in Figure 2, p. 39. Not all the acknowledgment types may be necessary for every sender's application; only the most appropriate ones should be used. The detailed implementation of acknowledgments should be based on a risk analysis of the transactions. For example, if the loss resulting from a lost or delayed message can be significant, the time allowed for receipt of an acknowledgment should be relatively short. Similarly, the greater the loss that would result from repudiation, the more extensive the use of acknowledgments should be. If errors in message content could trigger large losses, the recipient application acknowledgment should include validation information.

3.2.1 Sender's EDI System to Sender's Application

The EDI system should tabulate transactions received from the application since last acknowledgment (ack. #1, Fig. 2), recording for each transaction:

(1) the time it was received from the application,

(2) the number of bytes received from the application, and
(3) the status of the transaction.

The status of the transaction should be recorded as one of the following:

(1) queued for translation,
(2) translated error-free,
(3) failed translation and rejected,
(4) passed to the network,
(5) passed to recipient's mailbox (for systems using a VAN),
(6) downloaded by recipient (for systems using a VAN),
(7) acknowledgment received from recipient, or
(8) acknowledgment from recipient overdue.

At regular intervals, the EDI system should send a copy of the tabulation back to the application, which then reconciles the tabulation with its own records to ensure that all transactions were processed and dispatched to the network.

Each application should create and maintain a table of transactions that it passes to or receives from the EDI system. Each table entry should contain enough information to ensure that incorrect operation of the EDI system involving lost or mishandled transactions can be detected. The applications should be able to detect the failure of the EDI system to process outbound transactions in a timely manner.

3.2.2 Network to Sender's EDI System

VANs may provide senders with acknowledgments of receipt of EDI messages by their own and recipients' mailboxes (acks. #2A, #2B, Fig. 2). These reports provide audit trail information about the movement of messages and, as such, they provide evidence of transmission and receipt. This may be particularly important in a dispute caused by an attempt at repudiation. Note that the recipient's mailbox receipt report (#2B) returns through the network.

3.2.3 Recipient's EDI System to Sender's EDI System

Typically, transaction set 997 Functional Acknowledgment is generated automatically by the recipient's EDI system when a valid transaction set is received. The functional acknowledgment simply acknowledges receipt of the message, but it is not an operational "acceptance" of the intent of the transaction set. The TPA should be clear as to the meaning of a 997 with respect to each transaction set defined in the TPA. For example, it should not be taken to mean "acceptance" of a purchase order. Note that this acknowledgment (ack. #3, Fig. 2) also flows back through the network.

Functional acknowledgments should be assured to be generated by the EDI system in a timely manner. The TPA may call for a trading

partner to send functional acknowledgments for specific transaction sets within a specified time after receipt. Failure to acknowledge promptly will trigger an "acknowledgment not received" action by the sender, and require wasteful corrective actions by both partners. The system design should provide for the situation in which the sender initiates an "acknowledgment not received" action but later receives a positive acknowledgment from the recipient.

3.2.4 Recipient's Application to Recipient's EDI System

The recipient's EDI system can maintain a log of incoming transaction sets that it has passed to the applications. Periodically (e.g., daily), each application can acknowledge to the EDI system the number and types of transaction sets received and processed (ack. #4, Fig. 2). This will provide data necessary for the EDI system to detect lost transaction sets.

3.2.5 Recipient's Application to Sender's Application

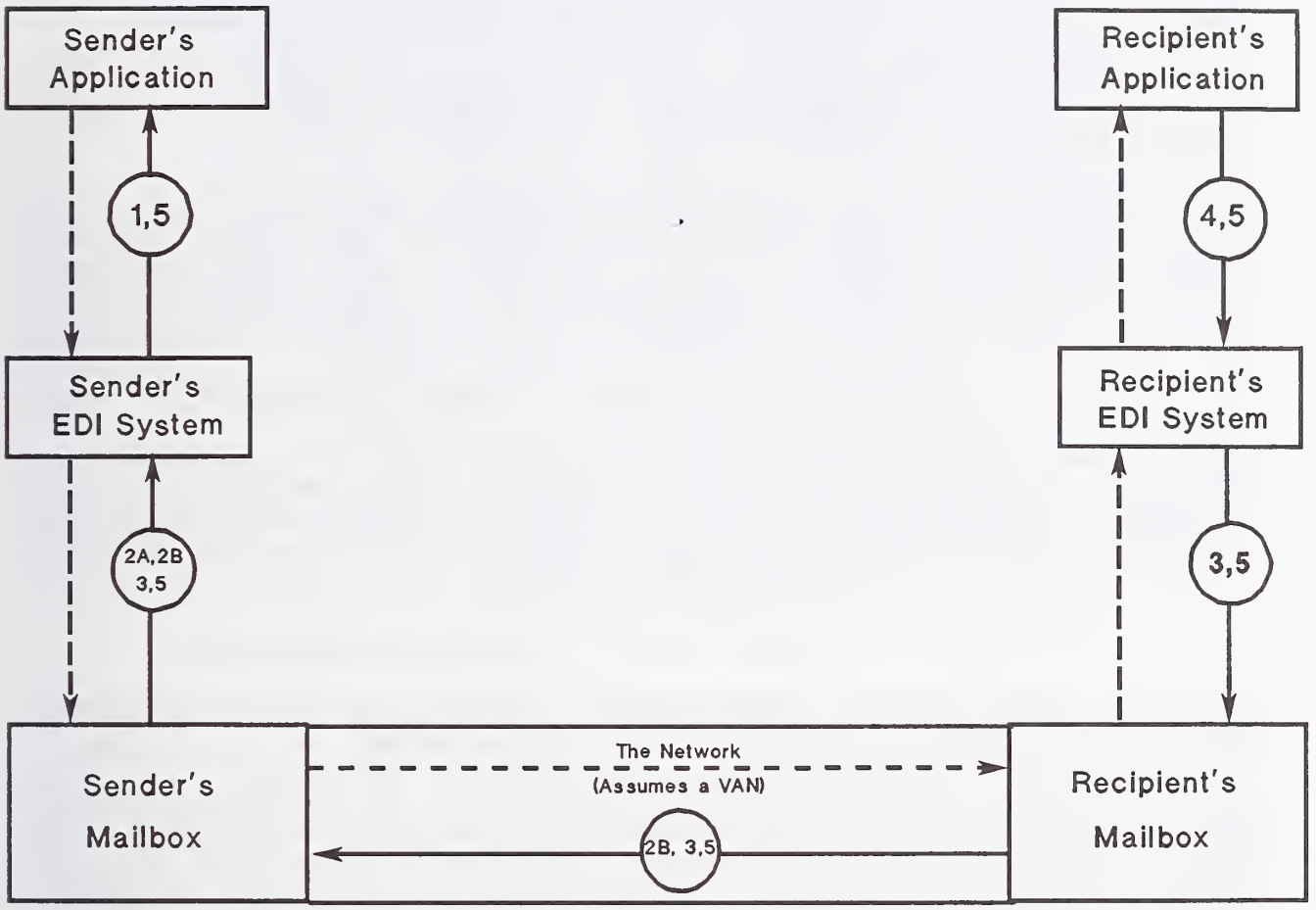
As specified by the TPA, the recipient's application that receives the translated transaction set acknowledges receipt, and indicates the action that the recipient is going to take. This acknowledgment is an action acknowledgment (ack. #5, Fig. 2), as distinguished from the 997 Functional Acknowledgment. An action acknowledgment transaction set might be, for example, an 824 Application Advice, 855 Purchase Order Acknowledgment, or 856 Ship Notice/Manifest. It is this acknowledgment that signals "acceptance or rejection" of the sender's transaction. Note that this acknowledgment also flows back through the network.

If an electronic document, passed to the recipient as an EDI transaction set, has been signed by an individual, the acknowledgment should include the imputed identity of the signer. The TPA should specify a time limit within which the sender, after receiving an acknowledgment, must question the identity if it is wrong. The acknowledgment may include information that the sender's application can use to verify that the information in the message was received intact without modification or corruption. For example, the acknowledgment might include hash totals of part numbers and monetary amounts, or it might indicate that a Message Authentication Code was confirmed.

3.3 Techniques for Applications

3.3.1 Sequential Numbering of Sender's Transactions for Each Recipient

Each application that generates sender transactions should assign an identifying number to each transaction, and include the number in the transaction set sent to the recipient. Transactions sent to a particular recipient should be sequentially numbered.



Acknowledgments shown by solid arrows
Message paths shown by dashed arrows

Acknowledgment Types

1: Status of sender's transactions

2A: Receipt by sender's mailbox

2B: Receipt by recipient's mailbox

3: Functional acknowledgment

4: Status of recipient's transactions

5: Action acknowledgment

Figure 2. Typical EC System Acknowledgments.

Case Study: A buying partner sent an EDI purchase order for 500 aluminum ladders to a selling partner. Because of a badly worded transmission error report, the buyer mistakenly concluded that the transaction set had not been received, and sent it again. Because the purchase order did not include a unique number, the seller could not detect the duplication. As a result, the seller fabricated and shipped 1,000 ladders to the buyer.

It is essential to include a unique sequence number in each outgoing operational transaction to ensure that the recipient can detect duplicate messages. Note, however, that the recipient cannot detect missing or out-of-sequence transactions unless the messages include sequence numbers that are unique to each recipient. Information messages, such as an RFQ (Request For Quotation) or price list update, probably do not require sequence numbers since the content of the message, e.g., an internal "publication" date, typically discloses duplicates. In other words, no harm is done if the recipient receives two copies of the same RFQ. Acknowledgments of sequence-numbered transaction sets should include the sequence number of the transaction set being acknowledged, so they do not require their own sequence numbers.

3.3.2 Testing For and Reporting of Duplicate Messages

Recipient applications should test incoming messages to detect duplicate messages, and report them to the sender.

The TPA should define the requirement for a recipient to detect duplicate messages and transaction sets, and the action that the recipient is to take when a duplicate is detected. A minimum default condition could be to ignore duplicate message. However, since a duplicate message is a symptom of an operating error or a system failure, it is good security practice to report the duplication to the sender, and for the sender to diagnose and correct the cause.

3.3.3 Error Handling

Applications should be enhanced to resolve error conditions, automatically if possible, or by generating exception reports for human resolution. It is important to ensure that error handling is complete and correct. The sender application must be able to detect and resolve correctly (a) failures to transmit messages, (b) failures to receive acknowledgments in a timely manner, and (c) acknowledgments that indicate that alterations to messages have occurred.

3.3.4 Testing For Invalid and Suspect Transactions

Recipient applications should perform traditional edit checks of incoming transactions, and should also verify the "reasonableness" of transactions.

There may have been significant reasonableness checking by human operators in the paper-driven system; this human oversight may not be completely documented. It is essential to identify all human oversight during the EC design and implementation phase, and to decide how that oversight is to be replaced with automated processing. For example, consider a recipient application that processes purchase orders from many other trading partners. The application might be modified to construct a profile of typical purchase orders for each of the other trading partners. As each purchase order is received, it could be compared with the sender's profile. If the purchase order falls outside the limits defined by the profile, it could diverted for review by an experienced staff member or to a computerized "expert system" for further analysis.

3.3.5 Assurance of Message Integrity

Both parties to a data interchange want reasonable assurance that the critical information included in a message when composed is unchanged when received. The concern for potential loss requires that, if an action is to be taken as the result of a message, the action is taken on the basis of correct data.

1) Use of Hash Totals

One common and elementary technique that helps assure message integrity is the inclusion of "hash totals" in the message. A hash total is a summation for checking purposes of similar fields in a file, such as fields containing part numbers, that would otherwise not be summed. This concept has been adopted for EDI. For example, the X12 850 Purchase Order transaction set allows the sender to include the sum of the value of the quantities added, as well as the total transaction amount. The TPA should require that hash totals be provided by the sender and verified by the recipient. Figure 3 illustrates the concept. This security measure is quite simple to implement.

Purchase Order No. 123-456

Quantity	Part Number	Unit Price	Total
3	1234	$ 123.45	$ 370.35
5	6678	$ 22.44	$ 112.20
8	7912*	145.89*	$ 482.55

*: Hash totals with no real-world meaning.

Figure 3. An Example of a Purchase Order With Hash Totals.

Verification of hash totals could be combined with reasonableness checking, as discussed in Section 3.3.4 above.

2) Secure Hash Standard

Hash totals only protect specific data fields in the transaction sets. It is also possible to protect an entire transaction set against undetected alteration or corruption. One way to do this is to use the Secure Hash Algorithm (SHA), specified in recently adopted FIPS PUB 180. The SHA accepts, as input, a message of any length in bits less than 2 to the 64th power, and generates a 160-bit output called a message digest. The SHA is called secure because it is not feasible to find a way to alter a message without altering the message digest. Thus, if a message is altered, the message digest calculated by the recipient will not match the digest attached to the message by the sender. FIPS PUB 180 includes a complete description of the SHA.

It is extremely unlikely that the body of a message and its message digest could both be corrupted accidentally such that the corrupted digest matches the corrupted message. Therefore the SHA will protect a transaction set against accidental alteration, but not against deliberate alteration. An intruder could deliberately modify a message, then calculate a new message digest and substitute it for the original digest. Thus, the message would appear unmodified to the recipient. If there is a significant risk of deliberate modification of a transaction set, then a more secure form of message authentication may be appropriate.

3.3.6 Digital Signature Algorithm

A digital signature provides additional security. It enables a message recipient to verify the originator of the message as well as the message content.

A Digital Signature Algorithm (DSA) which uses the SHA is currently being considered for adoption as a FIPS PUB. The DSA employs two cryptographic keys for each user. Each user has a public key that is known by all trading partners, and a private key that is kept secret. The message to be sent serves as input to the SHA; the output of the SHA operation is the message digest. The message digest and the sender's private key are used in a signing algorithm to calculate the digital signature. The recipient receives both the message and the digital signature.

A signature verification algorithm is used by the recipient to authenticate the signer. This algorithm uses, as inputs, the sender's public key, the received digital signature, and the message digest recalculated with the SHA from the received message. The verification algorithm recalculates one of two signature components. If the recalculated component matches the component as received, the signer is authenticated and the received message is

identical to that sent. If the signature fails to verify, the recipient must ask for the message to be retransmitted. The process is shown graphically in Figure 4, p. 44.

This public key technique has the advantage that it can be used in more than one trading partnership. Each user's key pair may be used for message interchange with any trading partner, and the private key need never be exchanged or revealed. However, for general implementation, a high-security administrative system needs to be in place. This system would provide secure distribution of private keys, and a trustworthy source of public key information. As of this writing, no such general system is available.

Non-cryptographic Originator Authentication: A simpler but less assured system for originator authentication is as follows. For each trading partner pair, the recipient generates unique lists of random numbers, and sends one list to each signatory in the sender's organization. The means of delivery used must protect the lists against compromise. Each time an individual wants to sign a message, that individual simply adds the next number on his or her unique list to the message, and then crosses off the number, making a note of the time and date it was used. The recipient verifies that the signature number on each message is the next number on the signatory's list, and the recipient includes the number on the message acknowledgment. If someone else in the sender's organization or an outsider gets access to the list and uses the next number, the acknowledgment will alert the authorized individual. This method, unlike the DSA, does not provide an integrity check for the whole message.

3.3.7 Message Confidentiality

If the risk analysis of a planned EC system shows that there is a significant possibility that sensitive messages will be disclosed while being communicated, and that the disclosure would be seriously detrimental, the messages should be encrypted. The cost to encrypt will include (a) purchase, operation and maintenance of cryptographic devices, (b) the cost to manage and distribute the cryptographic keys, and (c) the cost of any additional network data transmission capacity required (encryption usually increases the number of bytes in a message). The costs of protection and the potential losses due to disclosure could be factored into a QRA.

3.3.8 Audit Trails of Transaction Processing

To support non-repudiation, and facilitate recovery from errors and breakdowns, each application should maintain an audit trail of the processing of transactions.

If there is a significant risk of repudiation, the sender's application should maintain an adequate audit trail of the transactions that the application initiates. The audit trail should make it

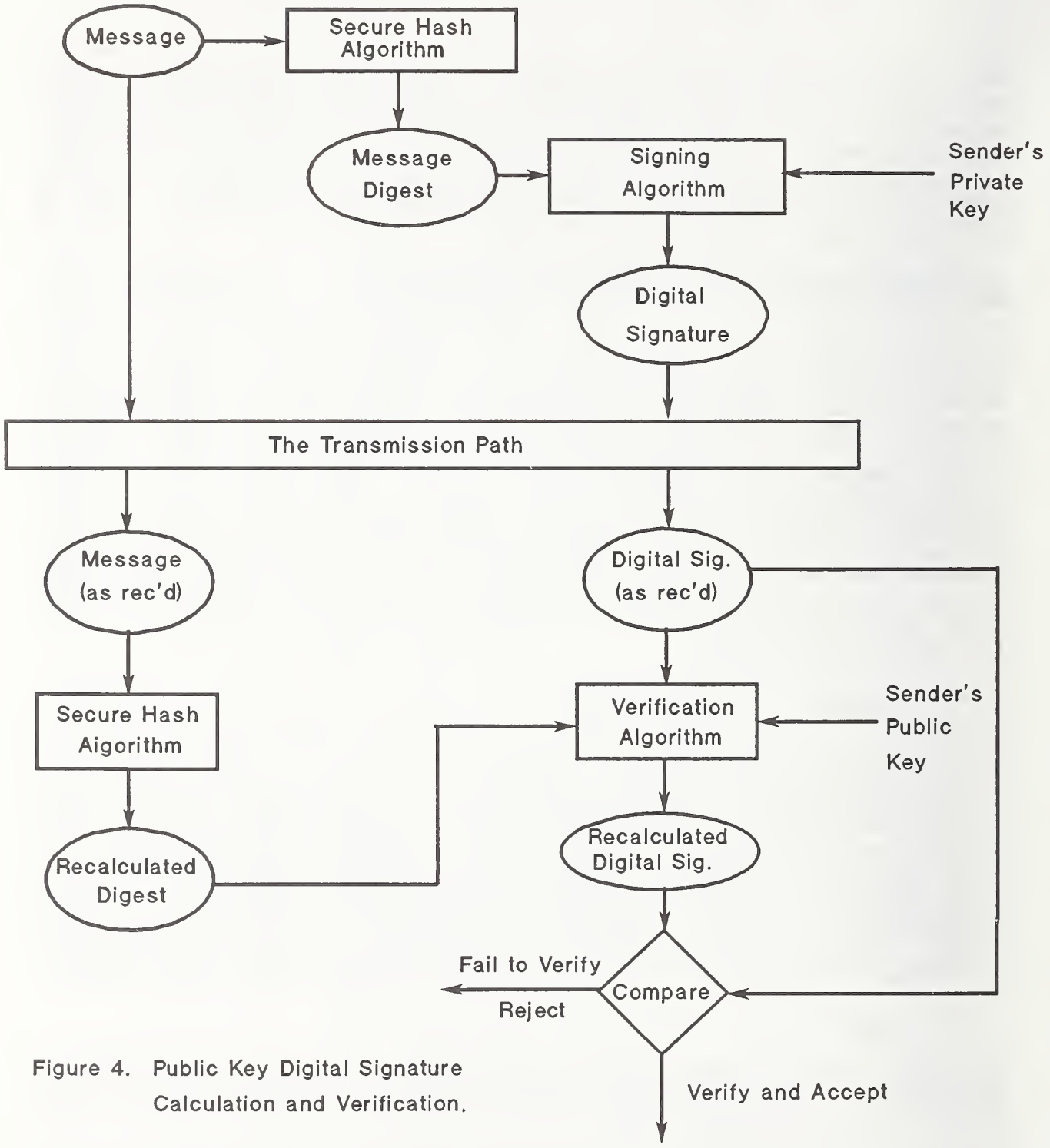


Figure 4. Public Key Digital Signature Calculation and Verification.

possible to confirm later the correct processing of questioned transactions, as for example when the recipient denies receiving a message. With adequate audit trails, the sender can show the sequence of messages sent to the recipient, including the repudiated message, with acknowledgment of delivery by the network, and receipt by the recipient. Likewise, recipient applications should maintain audit trails to be able to demonstrate timely processing and acknowledgment of transactions.

If the EDI system fails, a transactions audit trail can be used to determine which transactions were lost by the EDI system; these transactions would need to be re-entered.

3.4 Techniques for the EDI System

This section presents good security practices that apply generally to the EDI part of an EC system.

3.4.1 Use of Standard Transaction Sets

As noted in Section 1.5.1 of this report, FIPS PUB 161-1, Electronic Data Interchange, "adopts, with specific conditions, the families of standards known as X12 and EDIFACT." and requires the use of these transaction sets if they meet "the data requirements" of Federal agencies implementing EC systems. Since these standards have been carefully developed to ensure reliable, accurate EC, this requirement is a good security practice that all designers of EC systems should follow. Similarly, system designers should follow Section 8.4 of FIPS PUB 161-1 when designing a new transaction set when no X12-defined transaction set is yet available to perform a required function.

Section 10.4 of FIPS PUB 161-1 also specifies that X12 versions and releases should not be used after a period of time, provided that they are replaced by newer versions and releases. The intent of this requirement is to keep all trading partners current with similar versions, to minimize differences in software when a system of trading involves many partners.

3.4.2 Rejection of Invalid Transactions Without Correction

The EDI translation program should not attempt to correct invalid input from the sender's application.

The structure of the input from the sender's applications is communicated to the EDI translation program through tables, sometimes called maps, that relate data fields in the applications to the data elements of the corresponding EDI transaction sets. All applications must supply the required kind of data, for example, a number, a date, a text string, etc., or a default value for all the data elements. If an error occurs either because there is an error

in the map, or the application generates an invalid data field, the cause of the error should be identified and corrected. Attempts by the translation program to correct such errors will obscure the error condition, and the correction may not be made correctly. In particular, EDI system personnel should not under any circumstances edit input data. Otherwise separation of duties is lost, and corrections may be faulty. For all these reasons, invalid input should be rejected without exception.

The translation of transactions must be accurate and complete. A key step in the design of an EC system is to compare systematically the data fields in the sender's application output with the data elements defined for the target transaction set. If any data elements are missing, the sender's application must be modified to add the missing information, or suitable default values established. Finally, the action of the translation program should be tested exhaustively to validate the implementation of the program.

3.4.3 Maintenance of Audit Trails

The audit trails required to permit reconciliation by the application with the EDI system should be maintained, to support recovery from contingencies, and to support non-repudiation.

Facilities and procedures should be provided to report back to the applications the status of transactions processed. This enables the applications to detect lost, mishandled, or duplicated messages, and to recover from EDI system breakdowns.

Facilities, procedures, and controls, including back-up of input and output files and transaction logs, should be provided as required to ensure timely and accurate recovery from EDI system and network failures without omitting or duplicating messages.

The EDI system should maintain transaction logs that make it possible to confirm correct processing of questioned messages, as for example, if and when the recipient denies receiving a message.

3.4.4 Reliable Network Interface

The network interface must provide facilities to protect against duplication of messages by inadvertent retransmission of a message to the network. The EDI system must ensure that each message generated by the translator program is delivered only once to the network interface, and that every message received from the network is processed by the translation program only once.

The EDI system should monitor the response time of the network, and generate an alarm promptly if response falls below the expected level.

3.5 Techniques for the Network

The EC system design should include the required performance specifications for the network, including the level of required security. Whether the network is operated by one or more of the trading partners, or by a third party, the network should be treated as a separate entity. Thus, the same security and control considerations apply regardless of the reporting structure.

3.5.1 Network Acceptance Criteria

The trading partners should verify that a proposed network satisfies the EC system's technical specifications. In addition, the partners should be assured that the operation of the network will be in compliance with desired security and control procedures, and that the size and competence level of the network staff is adequate to deal with technical faults and emergencies, and requests for assistance from users.

3.5.2 The Network Usage Agreement

Acceptance of a network must include the execution of a network usage agreement with network management. A common network usage agreement should be used by all the trading partners to ensure that all partners have the same understanding of how the network will function as a part of the EC system.

If trading partners are using different networks that interconnect, it will be important for the usage agreements to consider the issues of joint data transmission, and joint contingency plans and recovery. Both networks must work together for the EC system to be operative.

3.5.3 Access Controls

A network should provide an effective system of access control and management. This system should include a system for assignment, change, and revocation of identifications and passwords used to access the network and its mailboxes. See also Section 3.6.

3.5.4 Treatment of User Messages

1) Editing of messages

Under no circumstances should network personnel be permitted to alter messages. This situation may arise specifically if a trading partner contracts with a VAN to perform the translation function.

Networks should apply checks to detect corruption of messages that occur before delivery to the recipient. However, it is not a good security practice to have network personnel edit messages that are rejected by translation software. If message corruption does

occur, the corrupted message should never be edited. Instead, the message should be restored from a back-up copy, or the sender should be asked to retransmit it. While this activity may delay messages, permitting network personnel to perform such edits is a major control weakness.

2) Retention of Messages

Retention of EDI messages by a network should be brief.

Networks should not retain back-up copies of messages any longer than is reasonably necessary to permit recovery from service interruptions. In most circumstances it should not be necessary to retain any copy of a message for more than a week. This practice minimizes the extent to which messages are outside the control of the trading partners.

3) Access To EDI Messages

Access to EDI messages by network personnel should be controlled.

Network personnel should not be able to access the text of EDI messages except as absolutely necessary to ensure proper technical operation of the network. The network should have controls that ensure that all such accesses are only made by authorized personnel, and are recorded.

4) Log of Messages

A network should maintain a transaction log of messages sufficient to permit later verification of the delivery of a specific message from a sender to a recipient to support non-repudiation. The retention period of these logs should satisfy legal requirements.

5) Controlled Delivery of Messages

A network should maintain for each user a table of other network users who are authorized recipients of messages. The network should reject messages addressed to non-specified recipients.

3.5.5 Protection of Network Terminations

Adequate physical security to network communications circuits should be provided at trading partner premises.

Every network is especially exposed to wire tapping and sabotage at the point where network communications circuits leave trading partner premises, since it is relatively easy to identify the specific circuits carrying the network traffic. Consequently, if there is a significant risk of wire tapping or sabotage, adequate physical access controls should be imposed on the network terminations located on trading partner premises.

3.5.6 Contingency Plan

A network should have a contingency plan that is consistent with the service reliability objectives. The contingency plan should be tested regularly. Since the conduct of EC is totally dependent on the operation of the network(s), it is essential to determine how operation will be resumed promptly if there is a network outage that is expected to last longer than the maximum acceptable service interruption. The risk analysis of an EC system should yield an estimate of the dysfunctional cost of a network outage as a function of the duration of the outage. An estimate should be prepared of the annual standby cost to maintain the capability to restore service using alternate facilities as a function of the time required to restore service. The optimum recovery time is probably the one with the lowest total of risk and standby costs.

Since the conduct of EC is totally dependent on the operation of the network, it is essential to demonstrate regularly the ability of the network to recover within the stipulated time. Regular tests of network contingency plans should be conducted. The usage agreement should specify how this testing is to be done. The trading partners should verify that the conduct and results of tests comply with the terms of the agreement.

3.5.7 Network Audits

A network should be subject to regular internal control audits by a technically qualified independent activity (not directly involved in the operation of the network) to ensure that appropriate controls and checks are in place, and that there is compliance with them. The usage agreement should specify how audits are to be conducted. The agreement should provide for the trading partners to receive copies of the audit reports directly from the audit activity, as well as copies of documents describing resolution of deficiencies enumerated in audit reports.

3.6 User Authentication and Access Controls

Logical access to the functions of an EC system should be controlled by a properly administered system of user authentication employing adequate facilities and personnel.

There are five EC system functions that should require user authentication as follows:

1) Access to the network to initiate transmit or receive EDI messages;

2) Access to the EDI system to control its operation or to update operating parameters;

3) Access to an application to control operation and initiate transactions;

4) Affixing an individual signature to a transaction; and

5) Initiation of an encrypted transmission.

As a minimum, the EC system design should provide for use of user IDs and passwords for each of the functions. If the risk analysis reveals an unusually high level of risk, consideration should be given to more secure techniques to authenticate individual users.

The security benefit of a password system depends entirely on the thoroughness with which passwords are administered. There have been numerous examples of how easily intruders have been able to break into systems where administration of passwords was weak. Appendix E of FIPS PUB 112, Password Usage, provides a detailed and authoritative discussion of password management. This appendix is based on the password management guidelines developed by the DoD Computer Security Center, and presents good practices for the administration of authentication based on user IDs and passwords. See also the more recent FIPS PUB 181, Automated Password Generator. Features presented in these documents should be applied to the daily operation of the EC system's authentication mechanism.

3.7 Electronic Document Management

A system of electronic document management should be provided such that all required business documents that are in electronic form are retained, stored, and indexed to satisfy operational, audit, and legal requirements.

The substitution of electronic documents for paper documents does not change the business and legal requirements for documents, whatever their medium. The development of the concept of electronic document management is a formal recognition of the requirement to be able to use electronic documents just as easily and confidently as paper documents. Several electronic document management concepts must be addressed during the design of an EC system:

1) Assurance of retention of all relevant documents.

2) An index system to allow prompt retrieval.

3) The dependability and effective life of storage media.

4) Protection of stored documents against unauthorized access, modifications, and disclosure.

5) Implementation of an audit trail including dates and times for recording additions, deletions, and alterations.

6) Document retention times and timely destruction of superfluous copies of documents.

3.8 Maintenance of Audit Trails

The discussion of electronic documents above makes it clear that record systems must be implemented to enable documents to be easily retrieved. Likewise it is important to be able to reconstruct the sequence of events when an error condition arises. Finally, EC can be expected to weaken the effectiveness of separation of duties as an anti-fraud control. For all these reasons, it is important to be sure that the applications and the EDI system create and maintain adequate audit trails and transaction journals. The system analysis and the risk analysis should both stress the need to identify the audit trail requirements.

In those cases where an audit trail is particularly valuable, consideration should be given to the use of techniques that chain records in sequence to prevent insertion or deletion of individual records. Such a requirement could arise in a defense against repudiation.

Since there may be substantial automatic resolution of error conditions, it is prudent to maintain a separate log of all such resolutions. If the error rate increases significantly, an exception condition requiring human intervention should be generated. Otherwise, recognition of a source of errors may be unduly delayed.

3.9 Contingency Planning

An adequate contingency plan for the EC system should be provided.

3.9.1 Development of a Cost-Effective Plan

The risk analysis of a planned EC system should yield an estimate of the expected losses (ALEs) associated with outages of each of the applications, the EDI system, and the entire EC system. If the TPA holds one trading partner responsible for the effects on other partners of an in-house service interruption, it will be necessary to include the effect of outages on other trading partners as well as the in-house effects. The ALE estimates should be stated as a function of the duration of the service interruptions. This information can then be used to identify the most cost-effective contingency plan for each application, the EDI system, and the entire EC system.

3.9.2 Plan Objective

The objective of the contingency plan is to ensure timely and accurate recovery from service interruptions, and events that

destroy hardware and data files. Timely recovery means that the maximum (worst case) outage will not cause excessive service interruption losses to any trading partner, and that performance standards in the TPA regarding timeliness will be met. Accurate recovery means that no transactions are lost or duplicated. By designing the contingency plan at the same time as the EC system itself, consideration can be given to the question of timely replacement of destroyed hardware, and the frequency with which files are backed up for on-site and off-site storage.

3.9.3 Functioning of the Plan

Adequate EDI system resources and personnel should be provided under the contingency plan to ensure prompt response to trouble and exception reports, and to requests for assistance from trading partners.

The size and competence level of the EDI system staff must be adequate to deal with emergencies and technical faults on time. Since EDI system failures have the potential to interrupt all EC transactions into and out of the organization, it is important to be sure that the EDI staff has the resources and training to deal effectively with emergencies. These considerations apply to a lesser extent to the operators of the applications.

In some cases, an EC system will involve a large, dominant trading partner and many small trading partners who participate at the request of the dominant partner. In such a situation, there are two important considerations.

The first is that an EDI system failure at the dominant partner may prevent timely performance by all the small trading partners. This is particularly important if the dominant partner is a Federal Government agency and the small trading partners make required filings through the EC system. The dominant partner should establish a policy at the time the EC system is introduced that defines how service interruptions at the dominant partner facility will affect the requirement for timely filings prescribed for the small partners. The policy should be included in the TPA.

The second consideration is that small trading partners may lack the breadth of in-house resources needed to deal effectively with exception conditions and emergencies that affect their EC systems. Since it is in the interest of the dominant partner to ensure smooth operation, the dominant partner should consider the value of providing a "help desk" service for the small trading partners.

As a minimum, the TPA should require all partners to maintain a roster of names (or functional titles) and telephone numbers of staff members trained and designated to deal with potential problems, and provide the other partners with a copy. These lists could be distributed as EDI messages that could be used to update

an automated "help desk" function that is a part of the EC system. Thus, a small trading partner who encounters a problem, can determine exactly who to contact for help.

3.9.4 Contingency Plan Tests

Regular testing of the contingency plans should be carried out to ensure that EC system performance commitments can be met. Experience with conventional data processing systems has shown that regular testing is essential to the effectiveness of a contingency plan. Tests perform three functions:

1) Staff members receive on-the-job training in the operation of the contingency plan.

2) Deficiencies in the plan are discovered, and corrective action is taken before an emergency arises.

3) Each trading partner can be assured of the ability of the other partner(s) to meet agreed to timeliness goals. Indeed, a requirement for regular testing should be a part of the TPA for just this reason.

3.10 EC System Compliance Audits

EC systems should be subject to regular internal control audits by a technically qualified independent activity (not directly involved in the operation of the EC system) to ensure that appropriate controls and checks are in place, and that there is compliance with them.

For all these reasons, the effectiveness of the security measures, controls, logs, and audit trails are even more important than they are for a traditional business system. Consequently, effective auditing to identify control weaknesses and failures to comply with controls is of increased importance.

Careful design and testing are intended to ensure that controls are adequate, but controls cannot reasonably be expected to work flawlessly when first put into operational use. Likewise, changing circumstances may weaken controls or lead to the requirement for new controls. Effective auditing will disclose such weaknesses and deficiencies.

The EC system implementation plan should ensure that the training of staff members during initial implementation is adequate to ensure both proper routine operation and, more importantly, correct responses to exception conditions. However, the initial training may not be completely effective, and personnel may be reassigned after initial training is completed. Finally, experience shows that, unfortunately, some staff members will violate the trust

placed in them under some circumstances. The nature of EC suggests that in some cases, fraud losses could be significantly higher than with traditional business systems.

For all these reasons, it is important to audit regularly for compliance with controls by staff members. Expediency is a poor reason for violating controls, and it may create a climate where dishonesty becomes more difficult to detect.

Verification of the integrity of the transaction logs and electronic document files is a key part of the audit program. These records are essential to the management of EC, the settlement of exceptions, and the resolution of repudiation by a trading partner.

The results of the EC system risk analysis should provide the basis for determining the appropriate level and detail of the audit program. This is done by balancing the expected level of losses as a function of the level (scope and detail) of the audit program against the cost to conduct the audit at each level. This analysis will provide an economic basis for the conduct of the audits by stressing the impact on security and efficiency.

3.11 Testing

The processing of all incoming and outgoing transaction sets should be thoroughly tested before live operation is begun.

Great care must be taken in the design and conduct of tests. Testing should proceed step by step. Tests should first verify that each application generates the expected output information for the EDI system. Next, the EDI translation software should be tested to verify that valid EDI transaction sets are generated for each of the application inputs. Following this, tests should be undertaken to verify that the EDI system constructs correct interchange envelopes. Finally, after both trading partners have completed the preceding tests, tests should be conducted together to verify correct end-to-end handling of EDI messages. Each transaction should be tested for: (a) boundary conditions of all input data fields, (b) error conditions such as invalid part numbers, dates, quantities, and prices, and null transactions, (c) failures to acknowledge, and (d) negative acknowledgments.

The system designers should not design or conduct the tests. Independent testers should design the tests based on the system specifications, with the goal of demonstrating that the systems work as intended, regardless of errors and omissions.

It is also critical to verify correct handling of potential overload conditions at month-end, quarter-end, and year-end when traffic levels may be abnormally high, and timeliness may be especially important.

Since EC between partners is likely to expand and evolve as the benefits of EC are realized, it is important to include permanent testing facilities in the design of systems. An EDI system should be able to distinguish test messages from operational messages.

Case Study: A EDI systems programmer, intending to perform a test, logged onto a network mailbox. He was surprised when the network automatically uploaded 1,200 pending messages into a test file instead of into the appropriate EDI system input storage area. The system programmer was not able to recover the messages, and it was necessary to have the messages retransmitted.

To avoid problems like this, VAN users may want to maintain a test mailbox to which system programmers can send test messages for subsequent retrieval. This is analogous to a local loop-back test on a communications circuit.

APPENDIX A: ABBREVIATIONS AND ACRONYMS

ALE	Annualized Loss Expectancy
ANSI	American National Standards Institute
ASC X12	Accredited Standards Committee X12
DISA	Data Interchange Standards Association
DoD	U.S. Department of Defense
DSA	Digital Signature Algorithm
EC	Electronic Commerce
EDI	Electronic Data Interchange
EDIFACT	EDI For Administration, Commerce and Transport
EFT	Electronic Funds Transfer
FIPS PUB	Federal Information Processing Standards Publication
IDs	Personal Identifications
NBS	National Bureau of Standards (now NIST)
NIST	National Institute of Standards and Technology
QRA	Quantitative Risk Analysis
RFQ	Request For Quotation
SHA	Secure Hash Algorithm
SOL	Single Occurrence Loss
TPA	Trading Partner Agreement
VAN	Value-Added Network
X12	See ASC X12

APPENDIX B: BIBLIOGRAPHY

American Bar Association, Section on Business Law, Electronic Messaging Services Task Force, "Model Electronic Data Interchange Trading Partner Agreement and Commentary," Business Lawyer, Vol. 45, p. 1717. 1990.

Baum, Michael and Henry Perritt, Jr. Electronic Contracting, Publishing and EDI Law. John Wiley & Sons, New York, NY. 1991.

Data Interchange Standards Association. 1993 DISA Publications Catalog. Alexandria, VA. 1993.

Gilbert, Irene E. Guide for Selecting Automated Risk Analysis Tools. NIST SP 500-174. National Institute of Standards and Technology. Gaithersburg, MD. 1989.

Helsing, Cheryl, Marianne Swanson and Mary Anne Todd, Computer User's Guide to the Protection of Information Resources. NIST SP 500-171. National Institute of Standards and Technology. Gaithersburg, MD. 1989.

National Bureau of Standards. FIPS PUB 65, Guideline for Automated Data Processing Risk Analysis. Gaithersburg, MD. 1979.

National Bureau of Standards. FIPS PUB 87, Guidelines for ADP Contingency Planning. Gaithersburg, MD. 1981.

National Bureau of Standards. FIPS PUB 112, Standard on Password Usage. Gaithersburg, MD. 1985.

National Bureau of Standards. FIPS PUB 113, Standard on Computer Data Authentication. Gaithersburg, MD. 1985.

National Institute of Standards and Technology. CSL Bulletin: Security Issues in the Use of Electronic Data Interchange. Gaithersburg, MD. June, 1991.

National Institute of Standards and Technology. CSL Bulletin: Digital Signature Standard. Gaithersburg, MD. January, 1993.

National Institute of Standards and Technology. FIPS PUB 46-2, Data Encryption Standard (DES). Gaithersburg, MD. 1993.

National Institute of Standards and Technology. FIPS PUB 161-1, Electronic Data Interchange. Gaithersburg, MD. 1993.

National Institute of Standards and Technology. FIPS PUB 180, Secure Hash Standard. Gaithersburg, MD. 1993.

National Institute of Standards and Technology. FIPS PUB 181, Automated Password Generator. Gaithersburg, MD. 1993.

Roback, Edward, NIST Coordinator. U.S. Department of Justice Simplified Risk Analysis Guidelines (SRAG). Gaithersburg, MD. 1990.

Saltman, Roy G., editor. Workshop on Security Procedures for the Interchange of Electronic Documents: Selected Papers and Results. NISTIR 5247. National Institute of Standards and Technology. Gaithersburg, MD. 1993.

Troy, Eugene F. Security for Dial-Up Lines. NBS SP 500-137. National Bureau of Standards. Gaithersburg, MD. 1986.

Wright, Benjamin. EDI and American Law: A Practical Guide. The Electronic Data Interchange Association. Alexandria, VA. 1989.

ANNOUNCEMENT OF NEW PUBLICATIONS ON COMPUTER SECURITY

Superintendent of Documents
Government Printing Office
Washington, DC 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued in the series: National Institute of Standards and Technology Special Publication 800-.

Name _____

Company _____

Address _____

City _____ State _____ Zip Code _____

(Notification key N-503)

The National Institute of Standards and Technology was established in 1988 by Congress to "assist industry in the development of technology . . . needed to improve product quality, to modernize manufacturing processes, to ensure product reliability . . . and to facilitate rapid commercialization . . . of products based on new scientific discoveries."

NIST, originally founded as the National Bureau of Standards in 1901, works to strengthen U.S. industry's competitiveness; advance science and engineering; and improve public health, safety, and the environment. One of the agency's basic functions is to develop, maintain, and retain custody of the national standards of measurement, and provide the means and methods for comparing standards used in science, engineering, manufacturing, commerce, industry, and education with the standards adopted or recognized by the Federal Government.

As an agency of the U.S. Commerce Department's Technology Administration, NIST conducts basic and applied research in the physical sciences and engineering and performs related services. The Institute does generic and precompetitive work on new and advanced technologies. NIST's research facilities are located at Gaithersburg, MD 20899, and at Boulder, CO 80303. Major technical operating units and their principal activities are listed below. For more information contact the Public Inquiries Desk, 301-975-3058.

Technology Services
- Manufacturing Technology Centers Program
- Standards Services
- Technology Commercialization
- Measurement Services
- Technology Evaluation and Assessment
- Information Services

Electronics and Electrical Engineering Laboratory
- Microelectronics
- Law Enforcement Standards
- Electricity
- Semiconductor Electronics
- Electromagnetic Fields[1]
- Electromagnetic Technology[1]

Chemical Science and Technology Laboratory
- Biotechnology
- Chemical Engineering[1]
- Chemical Kinetics and Thermodynamics
- Inorganic Analytical Research
- Organic Analytical Research
- Process Measurements
- Surface and Microanalysis Science
- Thermophysics[2]

Physics Laboratory
- Electron and Optical Physics
- Atomic Physics
- Molecular Physics
- Radiometric Physics
- Quantum Metrology
- Ionizing Radiation
- Time and Frequency[1]
- Quantum Physics[1]

Manufacturing Engineering Laboratory
- Precision Engineering
- Automated Production Technology
- Robot Systems
- Factory Automation
- Fabrication Technology

Materials Science and Engineering Laboratory
- Intelligent Processing of Materials
- Ceramics
- Materials Reliability[1]
- Polymers
- Metallurgy
- Reactor Radiation

Building and Fire Research Laboratory
- Structures
- Building Materials
- Building Environment
- Fire Science and Engineering
- Fire Measurement and Research

Computer Systems Laboratory
- Information Systems Engineering
- Systems and Software Technology
- Computer Security
- Systems and Network Architecture
- Advanced Systems

Computing and Applied Mathematics Laboratory
- Applied and Computational Mathematics[2]
- Statistical Engineering[2]
- Scientific Computing Environments[2]
- Computer Services[2]
- Computer Systems and Communications[2]
- Information Systems

[1] At Boulder, CO 80303.
[2] Some elements at Boulder, CO 80303.

U.S. Department of Commerce
National Institute of Standards
and Technology
Gaithersburg, MD 20899