Federal Grant
Electronic Commerce Committee

Research Grants EDI Implementation
Volume I

INTRODUCTION

February 1998

Contents

Chapter 1
Introduction

Electronic commerce (EC) is the employment of computer technologies to streamline business operations in ways that will reduce operating costs while at the same time improving business performance. EC has been widely used in the private sector for many years and is being used increasingly in government operations at all levels (federal, state, and local). The federal government has embraced a strong EC program in numerous business areas, including procurement, logistics, transportation, customs, taxation, and grants management.

FEDERAL GRANTS ELECTRONIC COMMERCE

Federal Grants Electronic Commerce Committee

The Federal Grants Electronic Commerce Committee (ECC) was established in 1994 by several grant-awarding agencies, including the Department of Defense (DoD), Department of Energy (DOE), National Institutes of Health (NIH), and the National Science Foundation (NSF).[1] Since then additional agencies have joined, and as of July 1997, the following agencies were participating:

- Department of Agriculture
- Department of Defense
  - Air Force Office of Scientific Research
  - Army Medical Research and Material Command (Acquisition Activity)
  - Army Research Office
  - Office of Naval Research
- Department of Education
- Department of Energy

[1] The ECC was established by a higher-level collaboration of many of these same organizations: the Business Practices Working Group (BPWG). That group addresses broader issues of grants management and how the organizations can work together to streamline business practices. See the *Federal Grant Electronic Commerce Committee: EC Project Plan, Second Edition,* May 1997, for more on the ECC and the electronic grants initiative.

- Department of Health and Human Services
  - Centers for Disease Control
  - National Institutes of Health
- Department of Transportation
- National Science Foundation.

Mid-1997 saw the federal electronic grants effort expand to form the Inter-Agency Electronic Grants Committee (IAEGC). This committee is sponsored by the Government Information Technology Service (GITS) board and the Federal EC Program Office. The ECC is participating in the IAEGC effort.

The goal of the ECC is to plan for and implement EC for grants administration. In this effort the participating agencies were to make use of common resources and employ standard approaches wherever possible.

The ultimate goal is to use EC throughout the entire grant life-cycle:

- Solicitation/announcement
- Application
- Award
- Postaward administration, including payment
- Closeout.

Since attempting all of this at one time was impossible, the ECC began its effort with the grant application.[2] It was also necessary to select the technical means for exchanging the application data.

EC and Grants

The ECC selected electronic data interchange (EDI) as the *initial* means for exchanging the grant application. That choice was based upon the broad Federal commitment to using EDI to exchange data with the government's trading partners in a wide variety of applications, including procurement, transportation, logistics, and finance. EDI is also a mature and stable technology ready to implement.

[2] Follow-up efforts include the grant award and invention reporting. Other related organizations have simultaneously been working on payment.

The ECC is also firmly committed to exploring and exploiting other forms of EC, including use of the Internet and the World Wide Web. Other ECC documentation will describe those efforts.

DOCUMENT PURPOSE

This document was written to support both federal agencies awarding grants and the organizations receiving federal grants with the testing and implementation of EDI.[3] It provides federal trading partners with the information needed to implement EDI for grants administration.

Volume 1 of this document was written to give both functional and technical analysts within the grants community an understanding of EDI, implementation conventions (ICs), and EDI implementation issues.

Volume 2 presents each federally approved grant IC and specifically provides trading partners with the information necessary to transmit grants management data using EDI. The ICs define the data and the locations of where the data will occur in the electronic documents.

VOLUME 1 ORGANIZATION

This volume contains three chapters in addition to this introductory chapter:

- Chapter 2–Introduction to Electronic Data Interchange
- Chapter 3–Understanding Implementation Conventions
- Chapter 4–EDI Implementation Issues.

It also contains five appendixes:

- Appendix A–Checklists for Translation Software and Value-Added Network
- Appendix B–Example Data Security Plan
- Appendix C–Part 10 of the Federal Implementation Guidelines for EDI
- Appendix D–Points of Contact and Web Page Information

[3] While committed to supporting EDI, the ECC is also committed to evaluating alternative or additional EC technologies. One of these clearly will be the Internet, and in late 1996 the ECC developed an initial list of data elements to use in an Internet grant application. The *EC Project Plan* documents both agency-specific EDI efforts and other EC technology approaches.

- Appendix E—Glossaries from the Federal Implementation Guidelines for EDI.

Chapter 2
Introduction to Electronic Data Interchange

This chapter defines EDI, describes its origin and growth, and discusses the technology and processes that it uses.

EDI DEFINED

EDI can be defined as the

> *computer-to-computer exchange of business information in a standard format.*

EDI acts as common language to get information from one computer system to another. In order to make use of that language, users must translate the information going to or from their computer application systems into or out of the EDI format. Offsetting the effort expended on translation are the benefits of flexibility: Each trading partner may use completely different and independent computer hardware, databases, and business procedures. The benefits are significant: paper and mail delays are eliminated, as are redundant data entry and the possibility of its attendant keyboarding errors.

However, more important than any of these advantages is the capability for the direct computer-to-computer exchange of data, using machine readable and processable information that does not require human intervention. With this method, business processes can be reengineered to simultaneously reduce cost and improve performance.

EDI relies on a public standard format that is application-neutral and developed by consensus across a wide spectrum of industries. It does not require the same software or hardware to be used on both ends of the information exchange.

The syntax for the data exchange come from standards developed by the American National Standards Institute (ANSI) Accredited Standards Committee (ASC) X12 or the United Nations Electronic Data Interchange for Administration, Commerce, and Transport (UN/EDIFACT).

ORIGIN AND GROWTH OF EDI

In many ways EDI started in the early 1960s when the Department of Defense began using electronic exchanges between its installations to manage items of supply. This system, known as the Military Standard Requisition and Issue Procedure (MILSTRIP), used 80 position records (IBM keypunch card images) to transmit information. The record position combined with the type of record defined the data. Within a few years of the inception of MILSTRIP, the rail industry established a cross-industry working group called the Transportation Data Coordinating Committee (TDCC), which used these and other concepts to exchange automated electronic information about railcars. This program was successful, and the TDCC concept—eventually to be called EDI—expanded into other transportation modes and industries.

By the 1970s, EDI and the TDCC standards had spread into industries such as warehousing, groceries, and pharmaceuticals. Some companies, in order to obtain competitive advantages, began to develop proprietary standards that only they and their customers could use. However, other participants felt that EDI would benefit everyone by being a broad and public standard. To that end, ANSI established the ASC X12 in 1979. Today, less than 20 years later, the X12 standards support nearly 250 types of business transactions, and tens of thousands of American businesses use it. EDI continues to grow and is being used increasingly in government and internationally.

EC AND EDI

The term “EDI” has been in use for more than 20 years. However, as the government began to use EDI, it also envisioned not simply paperless exchanges of data, but paperless offices. To represent this broader concept, the Defense Logistics Agency (DLA) in the early 1990s popularized the term “electronic commerce”. EC encompasses all the digital methods used to exchange all types of information needed to conduct business. Although the term “commerce” may suggest ordering and paying for items, the intended meaning covers the broad spectrum of all types of data exchange in a paperless environment.

EC can be defined as the

> *integration of electronic mail, electronic funds transfer, EDI, and similar techniques into a comprehensive, electronic-based system encompassing all business functions. It is the exploitation of information technology to improve commerce.*

EC includes such tools and methods as

- EDI,
- e-mail (including X.400 and X.435 exchange protocols),
- the Internet and intranets,
- bulletin board services (BBSs),
- on-line data access and query tools,
- workflow and forms software,
- groupware,
- imaging and optical character recognition (OCR),
- computer integrated manufacturing (CIM) and computer-aided design (CAD) tools and software, and
- contractor integrated technical information services (CITIS).

EDI, therefore, is just one of the EC tools available to an organization. Its focus is on structured business documents exchanged between trading partners. These documents include solicitations, proposals, awards, etc. They also encompass many initial documents such as solicitations and grant applications.

At the beginning of this chapter we provided a definition of EDI but there are others that could be made. Some view EDI as simply a data transmission syntax. Other see it as the set of the processes and technologies for moving data between organizations. Others focus on it as a business philosophy. It is all of these things and more. In the remaining sections of this chapter we will look at each of these three views in order to gain perspective on what you will be participating in.

EDI AS A SYNTAX OR DATA STANDARD

What Is ASC X12?

ANSI, mentioned earlier in this chapter, is a nonprofit private institute that promotes and maintains standards (The federal government participates in and supports the development of ANSI standards, but does not manage them.) ANSI maintains standards for several diverse items, including many in the data processing world—ranging from versions of the COBOL programming language to specifications for magnetic tape and to telecommunications protocols. Each standard is independently maintained by an ANSI Accredited Standards Committee. ASC X12 is the committee for EDI.

ASC X12 membership is open to everyone: companies, nonprofit organizations, government agencies, and individuals. The federal government is a very active participant. ASC X12 representatives meet three times a year; there are also interim subcommittee meetings and an annual conference. In these meetings standards are developed and revised to meet changing business needs and the expansion of EDI functionality. The secretariat for ASC X12 is the Data Interchange Standards Association (DISA). It arranges the X12 meetings, maintains the standards database, and disseminates the standards in paper and electronic form.

The standards are revised and published every December. Each publication carries a unique version and release number. For example, Version 3 Release 5 (003050) is dated December 1994, and Version 3 Release 6 (003060) is dated December 1995. Generally, the version and releases are upwardly compatible. It is important to know which version and release of the standards are being used for the data exchange to make sure everyone is working from the same standard.

The ASC X12 standards are actually a collection of specific standards for security, enveloping, and other matters, but at their heart are the Transaction Set Tables, the Segment Directory, and the Data Element Dictionary.

Transaction Sets

In the EDI environment, the electronic documents exchanged are referred to as transaction sets. They are assigned a name and a number for reference in the ASC X12 EDI environment.

Transaction sets represent the basic unit of business. In many senses the transaction set is the equivalent of a business form—a delivery order, an invoice, etc. A transaction set is a series of segments (similar to records in a database) which contain data elements (similar to fields in a record) to describe a standard format. Data elements use qualifiers to describe amounts, quantities, dates, and percentages. These qualifiers come before a value, date, or percentage to describe what the item represents—for example, actual costs, an early start date, or percentage complete.

The transaction sets define the structure of the data. The standard format makes it easy to program computer applications to talk directly with each other without any human interpretation of the information being exchanged.

A transaction set is identified by a unique three-digit number (e.g., 850) and a name (e.g., Purchase Order) and contains all of the data necessary to complete a

business transaction. Version 3 Release 7 (003070) contains nearly 320 transaction sets, representing a broad spectrum of business functions. A representative selection illustrates this diversity:

- 130—Student Educational Record (Transcript)
- 135—Student Loan Application
- 188—Educational Course Inventory
- 194—Grant or Assistance Application
- 810—Invoice
- 837—Health Care Claim
- 841—Specifications/Technical Information
- 850—Purchase Order
- 870—Order Status Report.

Segments

Each transaction set consists of a series of segments arranged in an order predefined by the transaction set table. A segment is a group of related data elements that is uniquely identified by an alphanumeric identifier and name. For example, the N1—Name segment contains six data elements identifying an organization (or individual) and its relationship to the transaction set (e.g., ship-to address). The DTM—Date/Time Reference segment identifies the date and time an event occurs (e.g., shipment date). Many segments like the N1 and DTM are generic and can be used in different transaction sets.

Data Elements

As stated above, segments are composed of one or more data elements—discrete pieces of information. The X12 data element dictionary contains more than 1,300 data elements, each uniquely identified by a number of up to four digits (for example, data element 373—Date, or data element 1226—Repair Action Code). It should be noted that many data elements are variable in length, and X12 EDI is a variable-length syntax. Also the X12 approach uses codes in one data element to define the type of data a second data element will contain. These codes are called *qualifiers*. These qualifiers come before a value, date, or percentage to describe what the item represents—for example, actual costs, an early start date, or percentage complete.

As mentioned previously EDI involves additional standard specifications, and this volume will discuss the X12 transaction set, segment, and data element syntax later in more detail. But suffice it for now to say that a primary responsibility of ASC X12 is to maintain these EDI standards.

EDI AS A PROCESS

The EDI standards define the means to structure business data, but it is another matter to get the data from your computer to your trading partner's. This section discusses this process.

The EDI Pieces

To make EDI work, the following hardware, software, and technical pieces must be in place:

- **Application systems—**These are the basic internal databases used by the trading partner to maintain their data (e.g., agency grant management system, trading partner financial system). Different trading partners will have different application systems, using different software; EDI will provide the common link.

- **Application interface programs—**In the paper environment your application system would have programs that accept data from terminals or PCs and from other programs to print forms or reports. For EDI transactions, these programs are replaced by others that receive EDI transactions, load your database, and extract outbound data from it to prepare EDI transactions. These programs are called application interface programs. They may be complex or simple, depending on the volume and complexity of the EDI business. They represent the most significant piece of programming that will have to be performed.

- **EDI translation software**—This software converts the various application interface program "flat files" (also known as user-defined files [UDF] or application files) and packages the data into an outgoing EDI message; or in reverse, the translation software formats the incoming EDI data received so it can be read into the application system.

  Translation software provides the means to communicate with trading partners, perform syntax or standards compliance checks, and manage all the data exchanges with various trading partners. Once the flat file is created and processed by the interface program, the EDI translation software imports the flat file and translates it into the X12 syntax. Most translation software will also establish the telecommunications session to send the transaction set to the recipient. Translation software is widely available

from commercial developers. You should take advantage of existing software rather than attempting to develop it in-house.

- **Computer hardware**—Hardware is needed to support the software described above. Depending on the volume and complexity of data, the hardware could involve any size computer: a PC, minicomputer, or mainframe system.

- **Telecommunications path—**This path is the actual physical connection needed to move the data among systems. In some commercial uses of EDI, a third party is used: value-added networks (VANs). VANs are private third-party data networks that supply electronic mailboxes and electronic connections that move the data from one location to another in a secure environment. While VANs have been very common in commercial practice for making EDI secure, stable, and convenient, they are not necessary for conducting EDI. For example, EDI transactions can go directly from sender to receiver using the Internet.

The Process

Using the grant application as an example and the basic EDI pieces described above, we outline here the typical steps that occur to actually transport data from one EDI user to another using the grant application transmission as an example:

1. A trading partner's application interface program pulls grant application data from their internal grants application database(s). This export routine produces a flat file for processing by the EDI translation software.

2. The export file (flat file) is run through EDI translation software. This software maps the data into the standard X12 format as required, and places outer "addressing envelopes" around the data.

3. The trading partner then transmits the EDI transaction to the agency via the Internet or other electronic means.

4. The receiving EDI server (which contains EDI translation software) sends a 997—Functional Acknowledgment (receipt notice) back to the trading partner to acknowledge receipt of the message. The EDI server also makes a backup copy of the message in the event it is necessary to re-create the exchange of data. This backup is an audit feature of the EDI process.

5. The receiving agency's EDI translation software opens the EDI message and typically creates a flat file.

6. The agency reads the flat file using its interface program, which can perform such functions as editing the data and routing it to the appropriate application program or location.

7. The agency's grants management application loads the data from the interface program and initiates the appropriate actions.

OTHER FEATURES OF EDI

From the simple outline above, it is not obvious that EDI is more than just a standard protocol that allows computers to talk with each other. It is also a standard way to do business electronically in a secure and auditable environment. EDI provides the following:

- **Receipt notices—**A receipt notice resembles a return receipt in the mail with a few extra features. It verifies that a customer received a message intact and that a deliverable requirement has been met.

- **Audit trail—**In an EDI environment, the user can trace a message throughout its journey from one point to another. In addition to providing a means of recreating a transmission in the event of a problem, this audit trail verifies message integrity; for example, it confirms that the data were not altered or intercepted during transmission.

- **Access control—**Passwords and other features help ensure that only authorized people have access to the information. This feature is very important when transmitting proprietary information.

- **Backups**—All EDI messages are archived in the event it is necessary to recreate a transmission. Backups can be a key factor if a dispute arises between a trading partner and the government.

- **Standardized document exchange method—**One of the goals of EDI is to eliminate agency-specific requirements for the different types of documents and deliverables that a government customer can request. Using direct connections for one type of document, diskettes for another, and paper for yet another increases the cost of delivering data. EDI eliminates these multiple delivery methods.

EDI AS A BUSINESS PHILOSOPHY

The organizations that will gain the greatest benefits of EDI are those that regard it as not just a technical means to exchange data, but a tool to support improved

business practices. EDI is best implemented as a part of an overall business process reengineering effort to simultaneously reduce operating costs while improving performance. EDI benefits are primarily of two types:

- Direct benefits, primarily from eliminating the paper
  - Eliminating redundant data entry
  - Reducing errors that result from multiple data entry
  - Reducing paper reproduction and storage costs
  - Reducing mail costs and delays
  - Reducing labor costs for processing the paper forms
- Indirect benefits (generally, these are harder to determine, quantify, and obtain but frequently are much larger in the end)
  - Reduced inventory and facilities
  - Evaluated Receipts Settlements (no invoicing)
  - Just-in-time delivery and direct delivery (no interim warehousing).

The message is not to simply "electronify" your forms, but use this opportunity to first determine organizational goals and strategies, and then automate and reengineer to meet those goals. Frequently this will mean crossing many company processes and organizational boundaries to integrate the data across as many of your business areas as possible.

Further, the success of the business function usually depends not only on your own organization but equally on that of your trading partner. Using a manufacturing example, an end-item manufacturer cannot perform well if its part supplier performs poorly, or if the distributors or retailers of its product perform poorly. In the grants administration business, a truly effective management process can occur only with the active cooperation of both the federal agencies and grant applicants.

SUMMARY

The above sections attempt to explain what is required to implement EDI. However, they may also have made EDI seem more complicated than it really is. It *will* require change in business operations, and it *will* require programming and testing. However, once implemented, it should be quick, seamless, and dramatically easier then all the data entry, reproduction, filing, and other paper-based efforts that we now take for granted.

Chapter 3
Understanding Implementation Conventions

The ASC X12 transactions sets (and their underlying segments and data elements) were designed to be very broad and generic, so they may be used by a wide variety of industries such as automotive, grocery, aircraft, etc. A purchase order for automotive parts may carry many different pieces of data than a hazardous waste delivery order. So something more is needed.

This section will focus on implementation conventions—their purpose, how they are developed and disseminated, and how to read them.

PURPOSE OF IMPLEMENTATION CONVENTIONS

X12 transaction sets represent the basic unit of business; for example, the transaction set 850—Purchase Order is exactly that; it is used to purchase something. However, like most X12 transaction sets, it is very generic so it can be used by a wide variety of organizations, and it contains many more data elements than any one user is likely to use. It also allows a variety of formats for some data. For example, dates can be stored in a number of day-month-year formats: yymmdd, ddmmyy, ddmmccyy, etc.

To put these X12 transaction sets to use another document called an *implementation convention* (IC) is used to define the specific use of an X12 transaction set within a specified trading partner community. ICs spell out exactly how a transaction set is used and narrows down the information required for a specific document. The IC will specify which segments and data elements will be used or not used. Where necessary it will define the format or structure of the data, and what user data is to be carried in any given X12 data element. This chapter will describe how to read an IC.

The ICs are important for the people who need to build the application interface programs among the various systems and the EDI translation software that is used to transmit the EDI messages between trading partners. They supply the details needed to describe record and field layouts and field sizes. The ICs can be used for compliance checking to ensure that an organization is sending the required information in the right format. They also identify which version and release of the EDI standard is used. In any event, the data directions provided by an IC must be followed by everyone in exactly the same way—or communications will fail.

GOVERNMENT USE OF IMPLEMENTATION CONVENTIONS

The federal government is initiating electronic commerce in many different business areas. Procurement is the largest area, but others include logistics, transportation, grants management, customs, and taxation. To the greatest extent possible the government is trying to standardize all of its programs for the benefit of both federal agencies and its trading partners.

The basic policy supporting federal implementation of EC is the Federal Information Processing Standard (FIPS) 161-2. It states that

- federal agencies shall employ EC to the greatest extent possible;
- the approved standards for electronic exchanges are ASC X12 and UN/EDIFACT; and
- in their use of ASC X12, agencies shall use an approved standard suite of transaction sets, and transmit data within them in accordance with implementation conventions.

FIPS 161-2 defines how the federal government is organized to formulate and approve implementation conventions.

FEDERAL EDI STANDARDS COMMITTEES

Two standards committees control and maintain the government's ICs. The DoD EDI Standards Management Committee (DoD EDISMC) functions at the DoD level. The Federal EDI Standards Management Coordinating Committee (FESMCC) operates at the federal level.

These committees ensure that government agencies use coordinated ICs that provide a single face to industry, ensure compliance to a standard set of procedures, and migrate various information pieces and functional areas to EDI. Because of this consistent approach, an organization that does business with the Navy, Air Force, Army, Department of Transportation, Department of Energy, or NASA can use the same electronic documents and formats for every government customer.

These standards committees also have various functional working groups to address EDI needs within the government. For example, the DoD EDISMC includes four working groups: Procurement, Transportation, Finance, and Logistics.

The National Institute of Standards and Technology (NIST) provides a registry of all approved ICs at the federal level. It also maintains a Web site from which users

can download federal ICs.[1] The Defense Information Services Agency performs a similar function for DoD-approved ICs that is also accessible through a Web site.[2]

A draft or prototype IC may be initiated at the DoD or Federal level. Each IC initially goes through a public comment, voting, and approval process within either the DoD EDISMC or the FESMCC. Federal agencies have a single vote in the approval processes. Once approved through the initial standards management committee the IC is also reviewed and voted upon by the other standards maintenance committee. For example, a Federal IC that is first approved within the FESMCC would then go through an approval process in the DoD EDISMC. Once an IC is approved through both of these standards committees, it becomes part of the federal IC repository. This ensures that the same electronic documents and formats will be used for every government customer.

IMPLEMENTATION CONVENTIONS TO BE USED IN THE GRANTS PROCESS

The grants community plans on the use of the ASC X12 transaction sets and implementation conventions as shown in the table below.

X12 Transaction Set No.	X12 Name	Implementation Convention for Grants Use	Transaction Flow
840	Request for Quotation	Solicitation	Agency to grantee
194	Grant or Assistance Application	Grant or Assistance Application	Grantee to agency
850	Purchase Order	Award	Agency to grantee
855	Purchase Order Acknowledgment	Award Acknowledgment	Grantee to agency
860	Purchase Order Change Request – Buyer Initiated	Award Modification	Agency to grantee
865	Purchase Order Change Acknowledgment/Request–Seller Initiated	Award Modification Acknowledgment	Grantee to agency
810	Invoice	Payment Request	Grantee to agency
820	Payment Order/Remittance Advice	Remittance and EFT[3]	Agency to grantee
194	Grant or Assistance Application	Progress Reporting	Grantee to agency
870	Order Status Report	Invention Report	Grantee to agency
997	Functional Acknowledgment	Functional Acknowledgment	Agency to grantee

[1] Secretariat for Federal EDI: http://snad.ncsl.nist.gov/fededi.

[2] DoD Electronic Commerce: http://www.acq.osd.mil/ec.

[3] Electronic Funds Transfer.

DEVELOPMENT AND APPROVAL OF THE ICS

The draft ICs for federal grants administration were written by the Logistics Management Institute (LMI). Data requirements for the ICs come directly from work done by the ECC.

The 194—Grant or Assistance Application IC was submitted to the FESMCC Federal Procurement Working Group (FPWG) and was subsequently approved by the FESMCC in January 1997. The award data requirements to be included in the Federal 850-Purchase Order IC, the 870—Order Status Report (Invention Reporting) IC, and updates to the Federal 194-Grant or Assistance Application IC are being prepared for submission to the FESMCC FPWG. All remaining ICs are on the ECC's future agenda.

WILL THE ICS CHANGE OVER TIME?

All standards must evolve over time or they will fail. It is likely in the first year of so of operation that lessons will be learned that will cause the operation to change. Changes in the underlying X12 standards may also affect the ICs (e.g., the date format and minimum/maximum change to accommodate the new century). Also, changes to ICs must be submitted to and approved by the FESMCC and DoD EDISMC.

However, within an additional 1–2 years, the effort will stabilize, and relatively few changes should occur that will cause significant reprogramming.

WHO NEEDS AN IC?

Every organization participating in the Grants EC effort must have an IC for each specific X12 exchange they wish to engage in with their trading partners. Programmers and systems analysts within the organizations will be the principal users. They will use it to program the translation software and interface programs.

HOW TO READ AN IC

This section describes the parts of an IC and how to read one[4]. Crucial to understanding an IC is knowing that its page format contains both material from the X12 standards and independent notes written by the IC developers. The standards data is in plain text (although frequently in bold or larger font sizes), while *all IC notes*

[4] Although Chapter 2 gave a brief overview of the EDI standards, it is assumed that you have at least accumulated a basic knowledge of the ASC X12 standards. If you are not familiar with the ASC X12 standards at this time, you should obtain formal training available from a number of sources including federal EDI resource centers, DISA, many consultants and seminars, ASC X12 conferences, and most likely your VAN and translation software providers.

written by the IC developer are in italic. It is the IC notes that will give you the primary direction on how to map a flat file being sent or received by your translation software. The standards information is primarily present to help you identify your location within the standards, although usage attributes for segments and data elements as well as syntax and semantic notes will be directly relevant.

Transaction Set Hierarchy

The transaction set hierarchy presented in a IC looks very much like the transaction set description in the X12 standards, but there are some subtle differences.

PRIMARY COMPONENTS

The following are the primary components of a transaction set hierarchy as presented in an IC (numbers in parentheses refer to labeled portions of Figure 3-1):

- The implementation convention number and name (upper left-hand corner). This is the specific title of the IC, as opposed to the X12 transaction set name. In the example shown in the figure, the IC title is the same as the transaction set number and name, 194—Grant or Assistance Application.
- (1) **ASC X12 Transaction Set Number and Name**
- (2) **Introduction**—This is a generic description of the transaction set purpose from the X12 standards.
- (3) **Notes—**These notes are part of the IC, not the X12 standards. They describe in general terms the use of the transaction set.

TRANSACTION SET TABLE

Next is the transaction set table, which consists of eight columns:

- (4) **IC Segment Usage** (no column header)
- (5) **Pos. No.**—The segment position within the table from the X12 standards. (X12 transaction sets consist of 1–3 tables: header, detail, and summary. Each segment has a unique number in the table, typically 010, 020, 030, etc. When changes in the standards occur, segments inserted between existing ones may be assigned intervening numbers such as 015, 016, etc.)
- (6) **Seg. ID**—The unique segment identification from the X12 standards
- (7) **Name—**The unique segment name from the X12 standards

Figure 3-1. First Page of the 194 IC—Transaction Set Table

194 Grant or Assistance Application (1)

Functional Group ID=GT

Introduction: (2)

This Draft Standard for Trial Use contains the format and establishes the data contents of the Grant or Assistance Application Transaction Set (194) for use within the context of an Electronic Data Interchange (EDI) environment. This transaction set can be used by organizations submitting applications for grants, cooperative agreements, and other assistance. These applications will typically include project, budget, personnel, descriptive, and other related data.

Notes: (3)

1. Organizations use this transaction set to submit a Grant or Assistance Application to a Federal Agency. This application may be in the form of an unsolicited proposal, or a response to a general announcement, a specific agency request, or an annual solicitation.

2. Federal Agencies use this transaction set to respond with proposed or approved budgets.

3. A single transmission of this transaction set shall be used to submit the application or budget for one project only.

4. In this convention, the term grant includes: grant award, research contract, and cooperative agreement.

Heading:

(4)	(5) Pos. No.	(6) Seg. ID	(7) Name	(8) Req. Des.	(9) Max.Use	(10) Loop Repeat	(11) Notes and Comments
Must Use	010	ST	Transaction Set Header	M	1		
Must Use	020	BGN	Beginning Segment	M	1		
	030	DTM	Date/Time Reference	O	>1		
N/U	040	LDT	Lead Time	O	>1		
	050	PWK	Paperwork	O	>1		
			LOOP ID - N9			>1	
	060	N9	Reference Identification	O	1		
N/U	070	L11	Business Instructions	O	>1		
	080	MTX	Text	O	>1		
			LOOP ID - NM1			>1	
Must Use	090	NM1	Individual or Organizational Name	O	1		
	100	N2	Additional Name Information	O	2		
	110	N3	Address Information	O	2		
	120	N4	Geographic Location	O	1		
	130	N9	Reference Identification	O	>1		
	140	PER	Administrative Communications Contact	O	>1		

- (8) **Req. Des.**—The Requirement Designator of the segment within the transaction set from the X12 standards. All segments are either mandatory (M) or optional (O). If a segment is mandatory in the standard, then in the

IC usage it is designated as Must Use. A segment that is optional in the standard may be Must Use, Optional (column is blank), or Not Used in the IC usage column (depending on the IC developer).

- (9) **Max. Use**—The maximum number of times a single segment may be repeated per the X12 standards. IC notes frequently restrict segment maximum use repetitions to be less than what the standards allow, but they may never permit them to be more. Note also that the standards sometimes specify the number of repetitions (e.g., N2 segment at position 100 has a maximum use of 2), while in other cases it is simply >1 (e.g., the N9 at position 130).

- (10) **Loop Repeat**—Similar to a maximum use, except it represents the number of times that a group of segments may repeat in a loop. The identification of the loop is indicated by a shaded horizontal bar before the first segment in the loop and is always the same as the identification of the first segment in the loop (e.g., the N9 at position 130). Vertical and horizontal lines identify the segments making up the loop. The loop maximum number of repeats is provided under this column. The IC notes frequently restrict the number of repetitions to less than what the standards allow, but may never exceed them.

  Loops may be nested within other loops. The outermost loop is considered to be loop level 1. Each succeeding loop is one level higher. Note that if the first segment in a loop is M, then the loop must be used at least one time. If the first segment is O, then the loop may be skipped entirely (unless the IC notes direct usage). Segments inside a loop that are marked M are mandatory only if the loop is executed.

- (11) **Notes and Comments**—Footnotes and comments about the transaction set or its segments from the X12 standard. Frequently not of direct use to the IC reader. The actual notes and comments appear after the table itself.

Seven of these eight columns are directly from the ASC X12 standards. Only the first column, IC Segment Usage (4), in the IC—which contains either Must Use, Not Used, or blank (meaning optional)—is directly derived from the IC.

The listing of segments shown in the segment hierarchy is the listing of all segments in the transaction set as defined by the X12 standards and in their proper order as defined by the standards. However, the next section of the IC, the segment page listing, contains only segments marked as Must Use or Optional (column is blank) in the segment usage column.

Segment Page Listing

Each segment the IC lists as used appears in the Segment Page Listing. The segments appear in the order defined in the transaction set. Those segments occurring more than once in different tables and loops will be displayed in each location. Each segment begins on a new page.

TOP PORTION

The top portion of the segment page consists of the following elements, listed horizontally down the page (numbers in parentheses refer to labeled portions of Figure 3-2):

- (1) **Segment—**The segment ID and name from the X12 standards
- (2) **Position—**The segment location within the transaction set table from the X12 standards. (This number, which is basically sequential, is the easiest way to find a segment in the Segment Page Listing after identifying it in the hierarchy.)
- (3) **Loop—**The name of the segment that begins the loop in which the segment occurs from X12 standards. If blank the segment is not in a loop.
- (4) **Level—**The table in which the segment occurs. It will be either the Heading (Table 1), Detail (Table 2), or Summary (Table 2 or 3, depending on the transaction set) from the X12 standards.
- (5) **Usage—**Whether the use of the segment is mandatory (per the X12 standards) or optional.
- (6) **Max Use—**The maximum use of the segment in that position from the X12 standards. This is the same as in the transaction set hierarchy.
- (7) **Purpose—**The X12 standard definition of the segments purpose. This will frequently be broader or more general than the segment will be used in the IC.
- (8) **Syntax Notes, Semantic Notes, Comments—**These are notes on how to use the segment or more often data elements within the segment as defined by the standards. Syntax notes are particularly important and all IC notes should be consistent with them. Comments are not part of the standard and are generally irrelevant to the IC. These areas may be blank.
- (8) **Notes—**These are the IC notes not from the standard. They provide the developer's specific instructions for using the IC. They are in italics.

Figure 3-2. Example of a Segment Page Listing

Segment: **DTM** **Date/Time Reference** (1)
Position: 030 (2)
Loop: (3)
Level: Heading (4)
Usage: Optional (5)
Max Use: >1 (6)
Purpose: To specify pertinent dates and times (7)
Syntax Notes: **1** At least one of DTM02 DTM03 or DTM06 is required. (8)
2 If either DTM06 or DTM07 is present, then the other is required.
Semantic Notes: (8)
Comments: (8)
Notes: *1. Use this DTM segment to identify the date the applicant's offer expires.* (9)
2. When the applicant organization is applying for Small Business Innovation Research (SBIR) or Small Business Technology Transfer (STTR) assistance, use to identify the date the for-profit company was founded.

Data Element Summary

(10)	(11) Ref. Des.	(12) Data Element	(13) Name	(14) Attributes
Must Use	**DTM01**	**374**	**Date/Time Qualifier** Code specifying type of date or time, or both date and time (15) 036 (16) Expiration (17) *Use to indicate the date this offer is withdrawn by the applicant organization from Federal Agency consideration for award.* (18) 145 Opening Date *Use only for SBIR and STTR applications to indicate the date the company was founded.*	**M ID 3/3**
Must Use	**DTM02**	**373**	**Date** Date (YYMMDD)	**X DT 6/6**
	DTM05	**624**	**Century** The first two characters in the designation of the year (CCYY)	**O N0 2/2**

DATA ELEMENT SUMMARY

The second portion of the Segment Page Listing is the Data Element Summary. This lists every data element contained in the segment that is used in the IC, in the order they appear in the segment from the X12 standards. (Within an IC Segment Page Listing, data elements that are not used are not printed, such as DTM03 and DTM04 on Figure 3-2.) The data element summary consists of five columns, the

fifth of which is subdivided into three additional areas (numbers in parentheses refer to labeled portions of Figure 3-2):

- (10) **IC Data Element Usage**—This is the left-most column, which bears no column label. It indicates whether a data element is Must Use or Optional (column is blank). This usage is assigned by the IC developer and is not a part of the standards, but it must be consistent with the standards. As mentioned above, Not Used data elements are not printed as part of the IC.

- (11) **Ref. Des.**—The reference designator from the standards. It is the segment ID concatenated with the numerical sequence of the data element within the segment.

- (12) **Data Element**—The unique number identifies the data element from the X12 standards. Most data elements occur in more than one segment. Its data element number will be the same regardless of which segment you find it in. However its reference designator (11) will vary by segment.

- (13) **Name—**The unique name for the data element number from the standards.

- (14) **Attributes**—The Attributes column consists of three components, all from the X12 standards:

  - *Usage*—The first is the data element usage as defined in the X12 standards. Each element is either M—Mandatory (Must Use), O—Optional, or X—Relational. For Relational data elements, the relationship between the data elements depends on the segment syntax notes. Usage of the data elements may depend on the usage of data in other data elements within the segment.

    Data elements marked M must be used and the left hand IC element usage must also be Must Use (e.g., DTM01 in Figure 3-2).

    Data elements marked O in the standards attributes may be marked Must Use by the IC developer in the usage column.

    Data elements marked X in the attributes may be marked in the IC usage column as Must Use (e.g., DTM02 in Figure 3-2) or Optional, except that such marking cannot violate the syntax or semantic notes.

  - *Data Element Type*—The second part is the data element type from the X12 standards. The types include AN—alpha-numeric (plus special characters), ID—an identification code list, Nn—fixed decimal point numeric (where n is the number of decimal places to the right of an implied decimal point), R—numeric (with a explicit decimal point), and others as defined in the X12 standards data element dictionary.

- *Minimum/Maximum*—The third part is the minimum/maximum length of the data element from the X12 standards.

ADDITIONAL DATA ELEMENT INFORMATION

Immediately below the actual data element names is more detailed information (numbers in parentheses refer to labeled portions of Figure 3-2):

- (15) **Data Element Description**—from the X12 standards.

- **Data Element IC Notes—**May appear immediately below the description. These notes, like all IC notes are in italic. Many data elements will not have notes if the usage of the element seems clear.

- (16) and (17) **Data Element Code Value and Description**—This information applies only to ID type data elements, and only those ID types for which codes appear in the X12 standards data element dictionary (e.g., the Zip Code data element is a type ID, but its codes do not appear in the standards). The code description (e.g., Expiration in Figure 3-2) appears to the right of the code value (e.g., 036 in Figure 3-2) and is a description of the code. (Many codes in the X12 standards have additional expanded code definitions that provide additional information. These are not displayed in the federal ICs.)

  ID Type Data Elements: For such codes the IC writer may have selected one or more of the available codes from the standards to be used in the IC. They are listed vertically down the page. *Only the listed codes may be used for implementation.*

  Alternatively, there may be no codes listed, but instead an IC note that says "Use any available code." In such a case *any code listed in the X12 standards for that data element may be used.*

- (18) **Code Notes**—These are IC notes for a specific code.

ADDITIONAL INFORMATION REGARDING INTERPRETING A FEDERAL IC

In the previous section we described the display of a segment layout. The transaction set hierarchy and the segment page provide all the basic information that programmers should need. However, this section provides some additional information regarding federal ICs, particularly regarding appendixes, override values, and hierarchical levels.

Appendixes

Transaction Set Hierarchies and Segment Page listings are the basic constructs of any IC. Some ICs may also contain one or more appendixes to assist programmers.

Override Values

Most X12 transaction sets have two or more tables. Table 1 typically is general information that applies to the whole business transaction. Table 2 generally contains details specific to a line item.

In general a segment used in Table 1 supplies information that

- is not applicable to line items. For example, the transmitting and receiving organizations for the transaction set are generally provided in Table 1 only.
- is detail information. However, it is the *same* for *all* of the line items and therefore becomes general. Placing this information in Table 1 simply avoids repeating it in every Table 2 for each line item and thereby reduces transmission time and costs.
- is part of a specific transmission that consists of only a single line item. In such cases X12 policy has been that where there are equivalent segments in Table 1 and 2, the segment in Table 1 is preferred.

It is the second circumstance above that creates most of the complexity in writing and reading an IC. The X12 syntax rules actually allow a Table 2 segment to override an equivalent Table 1 segment. Table 1 establishes the default value, but *if* the same code appears in the same segment of a specific Table 2 line item, then the detail value is overridden for that line item only.[5]

The Hierarchical Level

The 194 transaction set and some others contain only a very small table 1, and a table 2 that begins with an HL—Hierarchical Level segment. The HL segment defines the structure of the transaction set. The HL data element codes establish different structures depending on the business need. The HL loop in the 194—Grant or Assistance Application federal IC identifies the project organization, personnel,

[5] For sake of simplicity most federal ICs do not use this override capability and in some cases use only Table 2 for anything that relates to line item values.

technical data, and budget data associated with the grant application. Within the 194—Grant or Assistance Application, the HL segment allows for several structures:

- The Project loop is the first iteration of the HL loop. The Project loop is the highest level of the structure and provides Project-level information.
- The Project loop may contain a single subordinate Previous Award loop.
- The Project loop may also contain any number of subordinate Sub-project, Consortium, Key Person, Human Subject Care Group, or Animal Subject loops.
- Sub-project and Consortium loops may contain any number of subordinate Sub-project, Consortium, Key Person, Human Subject Care Group, or Animal Subject loops.
- Key Person loops may contain any number of subordinate Other Support loops.
- Care Group loops may contain any number of subordinate Medical Procedure loops.
- Animal Subject loops may contain any number of subordinate Animal Subject loops, but only if the subordinate loop contains a subset of animals of the same species.

The HL segment is an extremely powerful and flexible structure within the X12 standards, but it requires careful analysis in planning the programming.

Chapter 4
EDI Implementation Issues

This chapter describes the steps that are typically necessary for grant recipients to implement EDI and begin exchanging transaction sets with federal agencies. It also examines some of the technical, business, and legal issues that you will need to consider.

EDI IMPLEMENTATION STEPS

Implementing EDI involves the nine main tasks listed below. When your organization starts its planning, it may not require all the tasks listed; omit the ones you do not need. You may also choose to do these tasks in a different order.

- Get Management Endorsement
- Establish EDI Team
- Formulate Implementation Plan
- Identify Functional Requirements
- Resolve Technical and Operational Issues
- Set Up Connections
- Work with Trading Partners
- Testing and Production

Note that the following discussion emphasizes the effort necessary by a medium-to-large organization to implement significant business process reengineering (BPR) with EDI included. Smaller organizations and efforts may still do well to follow this approach, but each step will be smaller in scope.

Get Management Endorsement

Early in the effort each organization must decide the extent of reengineering it is determined to take on. At one end of the scale, it can obtain an EDI translator, key in its grant applications (for example), and transmit the results to the federal agency. When transmissions are received, they can be printed. This is the “no pain, no gain” solution: Investment costs are minimal, but benefits nonexistent. At the other end of the spectrum, an organization can invest heavily in an integrated grants management system (meaning *both* the business process and supporting data processing software and hardware) that will provide long-term savings and benefits to the organization; EC/EDI would be just a portion of what the system provides to the users.

Clearly such a reengineering decision is critical to the organization. Management must firmly support the plan by

- allocating staff, financial, and physical resources to the project;
- committing itself to an organization-wide approach, as EDI and BPR inevitably cross departmental boundaries, and coordination and cooperation must be ensured; and
- providing staff training and education regarding the effort. This is necessary to reduce staff resistance, solicit input and participation in the effort, and build acceptance of the end result.

Establish EDI Team

The EDI team keeps the process moving forward and addresses any policy, contractual, functional, or technical issues that may arise. Members of the team are the key people that work to create the EDI implementation plan and make sure all the resources are available. They set the goals, time frames, and any operational criteria.

The EDI team should also provide progress reports to upper management and other interested parties periodically (for example, monthly). These progress reports demonstrate that milestones are met and cost savings are realized.

The size and membership of the team will vary by the size of the project—for example, a payments-only project versus an entire grants payment system, or full system versus a prototype. The size of the organization and other variables will also have a bearing on the makeup of the team. An EDI team that would be representative of a medium or large research organization attempting to implement a full grants management system would include the following:

- Representatives from the functional organizations. This might include investigators, department heads, grants administration office staff, and financial staff. It should include professional and key clerical staff. These individuals must determine what is to be done and how to evaluate the results.
- Technical representatives from either or both departmental or central information systems groups. Technical staff must be responsible for application systems, EDI interface programs and translation software, telecommunications, hardware, and operations support.
- Representatives of special organizations such as audit, legal, and security groups.

An EDI team should include a leader who can devote significant time to the project and coordinate the actions across department boundaries. The representatives should be knowledgeable in their respective areas, forward-thinking, and open to change.

Formulate Implementation Plan

Like any other project, implementing EDI requires a plan to determine what needs to be done, who is doing it, when it is going to be done, and what kind of resources are required. The plan should also include some type of measurement criteria, such as milestones, to demonstrate progress.

A good place for an organization to start is to tailor to its needs a Plan of Action and Milestones (POA&M) and schedule. The organization can then supply copies of those to its trading partners for comment, revision, and agreement to proceed.

Identify Functional Requirements

The organization should identify the operational, business, legal, security, data, and technical issues that affect establishment of an electronic operating environment. The organization should devote significant resources to this task, since EDI is a business issue more than a technical problem.

The size of this effort is directly related to the extent of the organization's existing grants management automation and the project goals. Obviously, a large grant recipient organization with no existing system that is building a complete grants management system faces a substantial effort. An organization that is extending or improving an existing system may have much less to accomplish. Given today's information tools, a small or medium recipient can build a very sophisticated system for a modest amount.

For most implementation efforts, identifying the functional requirements will entail the following four subtasks:

- **Complete operating concept**—The organization develops a formal operating concept that describes, in detail, the data flows, trading partners, work methods, and procedures that it will employ in an electronic environment. This document should include business goals and expected functional improvements. It may include a cost-benefit analysis and success metrics or criteria.

- **Detail data requirements**—The organization identifies all data elements required. Recipients must analyze both data exchanged with federal agencies and data used only internally.

This document will be crucial in helping recipients understand what data the federal agencies will expect to receive or provide in the different transactions (application, award, etc.). Any reengineering effort must take these federal requirements into account.

Elements for internal use only will at least include those that manage the routing, processing, review, and approval of grant transactions within the organization.

For all data elements the organization will need to identify such things as the size and format of the element, organizations that create the element, and organizations that may revise it.

- **Determine modifications to application systems**—Key questions here include: Is a new system being built from scratch, or is an existing system being enhanced or expanded? Will the new system be built using in-house or contractor resources, or will it be purchased from a commercial source or from another recipient organization that has already developed a system?

- **Identify and resolve business, legal, and security issues**—The organization investigates and resolves all business issues. It also examines the legal and security requirements of EDI and its audit capabilities to ensure that it maintains the integrity of those functions in an electronic environment. Later sections of this chapter will discuss these issues further.

In defining and designing the functional requirements (as well as in all other steps), information from all possible sources should be gathered, but particularly from federal agencies and other recipient organizations that have already undertaken comparable efforts. Learn from their experience. Partnering can also be a very useful approach.

Resolve Technical and Operational Issues

The following actions must be completed before any data can be exchanged:

- **Provide a copy of applicable ICs to everyone involved—**In addition to the IC that defines the *structure* of the data, the recipient must be aware of any data *content* requirements. The content requirements generally are necessary data dictated by the receiving application or organization that are outside the scope of the IC (e.g., the federal government formats the date as ccyymmdd but your application stores it as mmddccyy). The IC identifies the version and release of the standard along with the information programmers require to build any application interfaces.

- **Identify the applications that will be used and any interface requirements—**Typically, an application system's input and output data must be mapped into a format that can be exchanged with the EDI translation software. This mapping is a one-time effort but may vary significantly in magnitude. An organization with low annual volumes that will use few transactions should develop simple interface programs. As the number of transactions and volumes increase, interface programs should become more sophisticated.

  The key functions of inbound interface programs are to edit data to ensure they will not "damage" the receiving application, convert formats where necessary, and route the data to the appropriate application. For outbound interface programs the key responsibilities are to ensure that the data conform to the appropriate federal IC.

- **Determine operations approach**—This includes moving the data from the business application system through the interface programs to the EDI translation software and to the telecommunications port. It will involve determining the EDI translation software and a hardware platform to operate it on. (A later section of this chapter will discuss translation software in greater detail.) Keep in mind that as you develop your grant system, other parts of your organization may already be conducting EDI and have components, which you can share. Many university administration offices conduct EDI to exchange student transcripts and loan data. State and local governments use EDI for procurement and payment.

Set Up Connections

The next step focuses on setting up the communications part of the process. The organization must first determine the preferred means. Most research trading partners will likely incorporate their EDI transaction into a mail message envelope and forward the transaction through the Internet. Other means include using a modem and a public telephone connection. This can be either direct with the federal agency or through a commercial VAN.

Regardless of the specific approach, it will require close coordination with the federal agency trading partner's telecommunications staff.

Work with Trading Partners

In a typical EDI implementation the development of a trading partner strategy is a major undertaking. For grant recipients, efforts by federal agencies have dramatically simplified the effort.

However, some work still must be done, as the various federal agencies are at different stages of implementation themselves and each has variations in how it has implemented EDI and the data that it collects.

The very first step in developing a trading partner strategy is to determine which federal agencies your organization does the most business with, and concentrate on those first. It is also wise to implement EDI with a single trading partner (agency) first and then expand on that success, rather than trying to accomplish too much all at once.

Similarly, you should review with the agencies which transactions you will attempt to implement first, either in full or pilot testing. Implementing the grant application will, in the long run, bring the greatest benefit to both your organization and the federal agency, but it represents both complex sets of data and an underlying business process. The grant award or the invoice/payment may be easier victories. Again, do not attempt everything at once.

As you move closer toward testing and implementation, many details will have to be worked out, down to exchanging the telecommunications path, computer telecommunications protocols, assigning technical representatives to plan the testing, and myriad other details.

Test and Production

The testing and production task involves several efforts required to field an EDI capability:

- Obtaining and installing hardware and software
- Developing interface programs
- Arranging for telecommunications services
- Developing detailed, updated operating procedures
- Training operators
- Testing, evaluating, and modifying the system.

Testing includes at least three different procedures:

1. **Basic (end-to-end) connection test**—This test verifies that the organization can send simple EDI messages through its EDI software to its trading partner's selected EDI server. During this test, the trading partner's translation software returns a 997—Functional Acknowledgment to verify that the sending organization can also receive EDI information. In addition, the mapped flat file (from the EDI translation software) is imported into the

end-user's system to ensure that all connections and security procedures are in place. The exchange between EDI systems can usually be completed in a matter of minutes or hours. Once everyone is satisfied with the results, the system is ready for the next step.

2. **Transaction set content test**—This test verifies that the four mappings (sender's interface, sender's translator, receiver's translator, and receiver's interface) were successfully completed. It also checks that the data content and format were what both sides expected. A good way to test this capability is to send old data (previously conveyed by paper or other means) to determine whether the organization is getting the same data through EDI. The data as displayed in the recipient's application system should be reviewed very carefully and compared to the data in the originator's system. This test should be run at least two or three times to verify that the system is working properly, resolve any problems, and highlight any potential pitfalls.

   This test demonstrates that all the pieces are in place. It helps determine whether anything needs to be fixed, if operating parameters need to change, and if all business requirements are being met with the IC. It also reveals any outdated paper-specific policies and procedures that may need to change to reflect the migration to an electronic environment.

3. **Parallel process**—During this test, the system moves to real time. The trading partner sends the data by the old method (paper or diskette) and by EDI for an agreed-upon period, usually at least three months. The implementation plan should include the target date the organization plans to begin and end the parallel process. The parties may want to notify each other in writing that the old process will stop on a given date.

Once testing is complete and the trading partners are ready to receive and send business information electronically, the organization is ready to use its EDI system in a production environment. After success in exchanging one transaction set with one federal agency, the organization can begin expansion to additional transaction sets and other agencies.

During this step, all the planning and implementation efforts come together. Along the way, lessons are learned about communications, the way EDI works, and the real benefits of EDI, including available metrics to show savings in time and money.

EDI TECHNICAL ISSUES

Translation Software

EDI translation software is widely available from many different vendors and for any size of platform, from PCs to mainframes. Translators are also available to support most operating systems, including UNIX, Windows, DOS, MVS, and others. The capabilities, features, and cost of the software vary significantly. PC packages are available for as little as $1,000 ($2,000–$5,000 is more common), while mainframe packages can range up to more than $25,000. The volume of transactions to be supported largely determines the size and cost of the software required. Most grants management systems will not have the volumes that require high-end technology.

One decision that may merit specific attention is the choice of platform the translation software is to run on (see the translation software checklist in Appendix A). Many organizations with large, complex, mainframe-based applications prefer to have their translation software on stand-alone mid-tier or personal computers. Doing this reduces the demand on hard-to-get mainframe computer time and programmer resources, creates a firewall between the EDI telecommunications and the mainframe, and improves access to the EDI resources for using other programmer options (i.e., different staff, consultants, etc.). Organizations running mid-tier computers or a file server environment may well have the translator run on the same platform, or offload it to a PC for many of the same reasons. Organizations operating on a PC would do well to retain the host application and the translator on the same platform, even if that means offloading other applications to a different machine.

You should explore your translator options extensively and carefully before committing to a particular translation package. In the case where a VAN is selected to provide your communications services, you may be encouraged by the VAN to use a specific translation software package which they have developed. If the VAN offers strong support for the package or price discounts, it is reasonable to accept this approach. However, be sure the package meets your needs. Any VAN should be able to work with any established translation software package.

Telecommunications Options

Implementing EDI will require decisions on telecommunications options for exchanging EDI transactions. This issue specifically refers to the actual physical connection needed to move the data among systems.

THE INTERNET

The Internet is one way to connect agencies, participating VANs, and the public sector that is either directly or indirectly connected to the Internet. It an inexpensive telecommunications path without the necessity of VAN services, and relatively simple means for exchanging any data, including EDI transactions, among trading partners. Furthermore, the Internet allows the use of many different data transmission protocols. The advantages of using the Internet are its low cost and ability to perform adaptive routing.

To conduct EDI over the Internet, a trading partner may contract with an Internet service provider (ISP) that provides Internet access and, if needed, software (such as Netscape); ISPs typically charge by the month. Many institutions can use their own existing Internet connections.

VALUE-ADDED NETWORKS

Value-added networks and value-added services (VASs) provide a variety of services. The most significant one is to simplify the telecommunications operations of an EDI capable organization. If an organization has only one trading partner, it would not generally need a VAN. However, as the number of trading partners increases, the complexity of telecommunications operations also increases dramatically (see the checklist for value-added networks in Appendix A).

Using a VAN means you establish direct telecommunications links only with your VAN. Your VAN worries about everyone else. Another convenience is the VAN's ability to act as a "store and forward" mailbox. If your application generates transactions once a day, then it can send them to the VAN when it generates them. They will remain there until picked up by trading partners at their convenience. If one of your trading partner's applications receives transactions only at a certain hour of the day, it can pick up mail from you at that time.

Almost all of the VANs have mutual agreements to forward transaction sets to each other for different trading partners. The reason that many EDI transactions flow from VAN to VAN is that each trading partner may have signed a contract with a different VAN other than the one their trading partner is using to meet its specific requirements.

In addition to supporting your telecommunications, VANs may offer to do the translation for you, archive the transactions that were exchanged, and other services as well.

The numerous VANs in business offer a variety of services and pricing structures. The Defense Information Systems Agency has approved more than a dozen VANs to participate in federal EDI. Note, however, that getting on the approved list means only that the VAN has demonstrated technical capability to exchange trans-

action sets. It is *not* an endorsement by the government of any VAN's offerings, service quality, pricing, or business practices.

Trading partners of federal agencies may use the VAN of their choosing, provided that it is a certified VAN or can exchange messages with one.

VANs and the Internet

An emerging area is combining the use of a VAN with the Internet. Some VANs are using the Internet as their communications pipeline. In other cases, Web forms are filled out by the trading partner and sent to a VAN, which translates and transmits the data using the EDI standard.

A more recent concept is to use the Web to download a Java "applet" that uses an IC to generate and display a form, which is filled out by the trading partner. The data are then converted to EDI and transmitted via the Internet directly or through a VAN, which may also perform the translation.

Point-to-Point Communications

The most basic communications approach is the point-to-point or direct connection between trading partners, either by dedicated line or through a dial-up network. This option would most likely be used if the organization only has one large trading partner. It requires close coordination of data exchanges between trading partners and becomes very complex as the number of trading partners increases.

No matter what method or software is used to develop or implement your system, we highly recommend that you take the open-systems approach (i.e., VANs or the Internet). That approach ensures that your system can interconnect with a variety of products.

EDI Business Issues

In addition to the technical issues described above, an organization implementing EDI must consider some factors related to its business operations.

Timing of Transactions

Implementation plans should include target time frames (the number of minutes or hours) to move the data from one point to another—for example, the time it takes to move data from the VAN to the EDI server to the end user. They should also include procedures for problem resolution and provide points of contact.

The significance of this issue is that most federal agencies follow a receipt, review, and award schedule. At the National Institutes of Health, for example, these schedules specify the application receipt dates for each type of grant, and the re-

view and award schedules (e.g., Scientific Merit Review, Advisory Council Review, and the Earliest Project Start Date). In the paper environment at NIH, the applications must be received by the specified dates. In the electronic environment, all transactions must be stamped with the date and time.

Furthermore, the timing issue requires decisions on when a business transaction will be made available to the trading partner. This involves decisions on warehousing, release, cancellations, and return, which depend on the type of business transaction.

Timing involves other factors, as well:

- **Legal issues**—Mailbox concerns to evaluate include consideration for postmark, utilizing VAN warehousing, utilizing the "recall" message time frame, timing of transaction acknowledgments, and timing of mail forwarding to recipient.

- **Technical issues**—The computer systems need to be able to respond in time. System changes might be necessary to accommodate the identified business needs.

Security

Security issues can be addressed with a security plan (a sample security plan is included as Appendix B). This plan spells out how and where the data move, who is responsible for what, what systems are used, what controls are used to manage the data, who has access to what, and what is considered to be receipt and acceptance.

A June 1991 Computer Systems Laboratory (CSL) bulletin on computer systems technology published by the National Institute of Standards and Technology (NIST) provided explicit guidance on EDI security. It directs that each activity implementing EDI attempt to satisfy five broad security requirements:

- **Message integrity**—The transmitting trading partner must ensure that all critical information transmitted is unchanged when received by another trading partner.

- **Confidentiality—**All trading partners must restrict access to EDI messages that contain personal, trade secret, or sensitive data.

- **Originator authentication—**The receiving trading partner must have assurance that the EDI message was transmitted by the named originator.

- **Nonrepudiation—**The trading partner establishing the EDI system must develop procedures to ensure that a binding proposal submitted by any trading partners cannot be denied.

- **Availability—**All trading partners must develop backup procedures for protecting important data in case of systems failure.

Depending on the type of data and its importance to your operations, security should be as strong as necessary to protect you and your trading partner. There are many approaches to securing a system. The typical approaches below can be used singularly or as a package.

- **Data encryption**—Data are encoded by a software encoder into unreadable scrambled text. The receiving party would unscramble the message to plain text.

- **Call-back modem**—The receiving party calls the sender back at a predetermined phone number before transmission occurs.

- **Passwords**—The sender protects data with a password that must be supplied to the system before the receiving party obtains access to the data.

- **Access codes**—Similar to passwords; the receiving party must enter certain codes to access the data.

- **Terminal source security**—This involves software coding that prohibits data from being sent or received except from a specific logical or physical device. If the device is not used, then the software erases the screen. In addition, this can be set up with a time slot. If transactions are attempted outside of the specified time slot, the software will cease operating.

- **Electronic authorization**—This area is a growing field and includes such increasingly commonplace elements as voice recognition, palmprint identification, and hand geometry.

Each of these elements, in combination with physical security, can effectively deter unauthorized entry to systems.

Recovery Procedures

The EDI plan must establish backup procedures for retransmitting EDI messages. Your organization must do the following:

- Establish backup and recovery procedures for computer system or transmission failure.

- Establish a maximum number of retransmission attempts following a text transmission error, to minimize communication costs for bad connections.

- For real-time transactions, establish 24- to 48-hour immediate access backup as a minimum.

- For batch transactions, establish 1- to 2-week immediate access backup as a minimum.
- In either case, specify some type of archival storage where the data is backed up and stored more permanently. The permanent archives and supporting system should provide for recovering a specific EDI message from the archives and retransmitting it.
- Ensure that the backup recovery system is thoroughly documented, to allow anyone with the proper authority to access the system to retransmit data.

Use of the Functional Acknowledgment

The 997—Functional Acknowledgment transaction set can provide a level of automation in backup and recovery. Once the 997 is received, the original EDI message can be archived, regardless of the normal archive timing.

The system could be designed with some flexibility. The use of the 997 could then vary based on business requirements. It might be appropriate to send and receive functional acknowledgments according to trading partner, the type of transaction, some combination of the two, or some other variable unique to your EDI requirements.

Your level of risk must be known when considering justification for the additional costs of including a flexible 997 component in your EDI system.

EDI LEGAL CONSIDERATIONS

In addition to technical and business considerations, EDI involves some issues with legal implications.

Trading Partner Agreements

A trading partner agreement (TPA) spells out the administrative details related to the exchange of data such as responsibilities, points of contact, transaction sets used, ICs used, version and release of the standards used, and specific contracts.

The federal government has set up a Central Contractor Registration (CCR) site on the Internet[1]. The purpose of the CCR process is to facilitate registration by a commercial company as a trading partner with the federal government. All federal government vendors, suppliers, and trading partners should be registered in this central database. The government will use this information as part of the information exchange and simplify this administrative step for the organizations.

[1] "The Central Contractor Registration Process," http://ccr.edi.disa.mil/.

Authentication

To ensure that EDI messages are authentic, an organization can use one or more of the following techniques:

- Require that every trading partner send an acknowledgment for each EDI message it receives. Most EDI translation software packages include this feature as an option.
- Require that VAN message status reports be sent to both the sender and recipient of EDI messages.
- Require reference numbers or passwords, known only to the sending and receiving trading partners, within the EDI message.

Digital Signature Standard

Some transactions (for example, those that obligate funds) may require a signature conveying the appropriate authority for the transaction and authenticating the identity of the signer. Instead of a traditional written signature, electronic transactions can meet this requirement with a digital signature.

Federal Information Processing Standards Publication 186 (FIPS-186) specifies a way to generate and verify such digital signatures.[2] Its digital signature algorithm (DSA) generates a pair of large numbers—the digital signature—represented in a computer as strings of binary digits. The digital signature can be used to verify the identity of the signatory and the integrity of the data.

HANDLING POTENTIAL SYSTEM PROBLEMS

The EDI system itself should manage some problems that could occur. For example:

- A trading partner's computer won't answer when your computer calls to pick up or deliver EDI messages.
- A bad connection causes too many retransmissions.

In addition, the EDI system should notify someone when a predetermined threshold number of errors are encountered.

[2] National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, FIPS-186, 19 May 1994, available at the Internet site http://csrc.nist.gov/fips/fips186.txt. The FIPS series, published by NIST, is the official series of publications on standards and guidelines promulgated under Section 111(d) of the Federal Property and Administrative Services Act of 1949 as amended by the Computer Security Act of 1987, Public Law 100-235.

Disaster Recovery

Disaster recovery also becomes correspondingly critical to the amount of business that is conducted through the EDI channels. Consider the consequences to you and your trading partners if you were suddenly unable to telecommunicate for a week. Have a plan in place to deal with extreme problems, such as the total loss of a data center or computer system, or the loss of a phone company switching station that services your area.

Audit Considerations

Long-term backup and audit capabilities should also be part of the EDI system. The EDI translation software will furnish some measure of backup and audit tracking. An organization may elect to implement additional backup measures for longer-term data storage.

Audit trails need to be established in any exchange of business information. These trails need to provide a means to reconstruct total transaction sets in the event of failure somewhere in the process. The auditing system should be able to do the following:

- Ensure that all records or documents are sent and received;
- Document and report all errors and their causes
- Record the start and stop time of communication for both parties
- Provide user reports for record and document counts.

Errors found in generation of the user reports should highlight the number of files expected to be received by the EDI system versus the number of documents counted.

EDI SKILL REQUIREMENTS

Implementing EDI will mean using new skills. Here are some of the things this change will require in your organization:

- Committing upper management to support the effort, because there will be bumps in the road
- Committing staff to learning the EDI process and understanding the standards and technologies used
- Programming to develop and maintain the interface programs between host application software and the translations software

- Programming to manage the translation software
- Finding technical staff with telecommunications skills
- Programming to ensure proper auditability and archiving of historical data
- Supplying hardware space to support the translation software (this can be on the application platform or other hardware), and hardware to support telecommunications (minimally a modem board on a PC and a telephone line)
- Providing technical and operations staff to manage error processing, archiving, adding trading partners, etc.

The complexity and amount of time required to support the EDI process depends heavily, of course, on the volume of EDI transactions, the number of different transaction sets, and the number of trading partners. The greatest amount of the work occurs in the initial design, development, and testing. Once in routine operation, the support workload drops significantly.

Appendix A
Checklists for Selecting Translation Software and Value-Added Networks

Throughout this document we have discussed the importance of selecting the most appropriate EDI translation software and VAN to support your EDI operations. This appendix describes some of the criteria in selecting translation software and a VAN, and provides two checklists which may be valuable in assisting you in evaluating alternative software and services.

EXAMPLE CHECKLIST FOR TRANSLATION SOFTWARE

The form on the next two pages provides an example list of items you can use to determine whether an EDI translation software package meets your business requirements. Please use this checklist as a place to start, and modify it as needed to fit your business environment. For the top two or three vendors you select, try to get an evaluation copy of their software to confirm which one best fits your needs.

Example Translation Software Checklist

How To Use This Form:

1. Circle a priority rating for each feature important to you. (1 = "must have," 2 = "nice to have").
2. Ask the vendor about the features provided. Mark the Yes or No checkbox accordingly.
3. Calculate the score by following these steps:
   a) Look for all the checked Yes boxes. In the Score column, enter a 10 for Priority 1 items and a 5 for Priority 2 items.
   b) Look for all the checked No boxes. Enter a zero in the Score column.
   c) Sum the numbers in the Score column.
4. The higher the score, the more closely the vendor meets your operating requirements.

Name of company _____
Contact name and phone number _____

	Priority Rating		Yes	No	Score
Company background—acceptable profile (Consider years in business, number of installed systems, industry-specific experience and support, involvement in standards process, etc.)	1	2	❒	❒	_____
Communications capability					
Value-added network independent	1	2	❒	❒	_____
Communicate with all VANs	1	2	❒	❒	_____
Provide VAN linkup administrative help	1	2	❒	❒	_____
Protocols supported					
Asynchronous	1	2	❒	❒	_____
Bisynchronous	1	2	❒	❒	_____
X.400 enveloping	1	2	❒	❒	_____
Security such as encryption	1	2	❒	❒	_____
Standards supported					
ASC X12, what versions and releases	1	2	❒	❒	_____
UN/EDIFACT, what versions and releases	1	2	❒	❒	_____
Operating environments					
Mainframe (and specific operating system)	1	2	❒	❒	_____
UNIX (hardware specific)	1	2	❒	❒	_____
PC (DOS, WIN 3.x, WIN 95), OS/2, or MAC	1	2	❒	❒	_____
Local-area network	1	2	❒	❒	_____
Single- or multiple-user system	1	2	❒	❒	_____

	Priority Rating		Yes	No	Score
Software capabilities					
All transaction sets	1	2	❒	❒	_____
Binary capability	1	2	❒	❒	_____
Compliance checking	1	2	❒	❒	_____
Management logs, audit capability	1	2	❒	❒	_____
Generate functional acknowledgments	1	2	❒	❒	_____
Automatically create trading partner profiles	1	2	❒	❒	_____
Operate in background mode	1	2	❒	❒	_____
Tailored transactions or hard coded	1	2	❒	❒	_____
Speed acceptable	1	2	❒	❒	_____
Edit process acceptable	1	2	❒	❒	_____
EDI to fax or fax to EDI	1	2	❒	❒	_____
Integration capabilities					
Mapping capabilities	1	2	❒	❒	_____
Flat file methods—in/out bound, fixed/variable	1	2	❒	❒	_____
Data-entry options available	1	2	❒	❒	_____
Fills in additional data	1	2	❒	❒	_____
Methods to link with other application systems	1	2	❒	❒	_____
Security options					
Passwords	1	2	❒	❒	_____
Data encryption	1	2	❒	❒	_____
User support					
Easy to install	1	2	❒	❒	_____
Documentation readable/useable	1	2	❒	❒	_____
Upgrade policy acceptable	1	2	❒	❒	_____
User group exists	1	2	❒	❒	_____
Training services—on site/their facilities	1	2	❒	❒	_____
Help line					
Available __ hours or from ___ a.m. to ___ p.m.	1	2	❒	❒	_____
Available __ days per week	1	2	❒	❒	_____
Reach knowledgeable person on first call	1	2	❒	❒	_____

Total score ☐

EXAMPLE CHECKLIST FOR VALUE-ADDED NETWORKS

The form on the next two pages provides an example list of items that you can use to determine whether a value-added network service provider meets your business requirements. Use this checklist as a place to start, and modify it as needed to fit your business environment. Be sure to confirm that the vendor is a federally certified VAN.

Example Value-Added Networks Checklist

How To Use This Form:

1. Circle a priority rating for each feature important to you. (1 = "must have," 2 = "nice to have").
2. Ask the vendor about the features provided. Mark the Yes or No checkbox accordingly.
3. Calculate the score by following these steps:
   a) Look for all the checked Yes boxes. In the Score column, enter a 10 for Priority 1 items and a 5 for Priority 2 items.
   b) Look for all the checked No boxes. Enter a zero in the Score column.
   c) Sum the numbers in the Score column.
4. The higher the score, the more closely the vendor meets your operating requirements.

Name of VAN _____

Contact name and phone number_____

	Priority Rating	Yes	No	Score
Access method				
Local number	1 2	❒	❒	_____
Toll-free 800 number	1 2	❒	❒	_____
Protocols supported				
Asynchronous	1 2	❒	❒	_____
Bisynchronous	1 2	❒	❒	_____
X.400	1 2	❒	❒	_____
X.25	1 2	❒	❒	_____
Standards supported				
ASC X12	1 2	❒	❒	_____
UN/EDIFACT	1 2	❒	❒	_____
Data security				
Data encryption	1 2	❒	❒	_____
Passwords	1 2	❒	❒	_____
Audit trace	1 2	❒	❒	_____
Connections				
All domestic VANs	1 2	❒	❒	_____
All international VANs	1 2	❒	❒	
DOD-certified VAN	1 2	❒	❒	_____
Proprietary e-mail products of choice: Novell, Microsoft, Lotus cc:Mail, etc.	1 2	❒	❒	_____
Work group or forms software of choice	1 2	❒	❒	_____
Internet	1 2	❒	❒	_____
Information services of choice	1 2	❒	❒	_____

	Priority Rating	Yes	No	Score
Pricing structure and figuring costs				
By character (get figure for sample document)				
Fees for interconnection to other VANs				
Installation fees				
Annual subscription fee				
Connect charges				
Monthly charges				
Mailbox charge				
Volume discounts available				
Flat fee available				
Total costs:				
High	1 2	❒	❒	_____
Low	1 2	❒	❒	_____
Additional services provided				
EDI to fax or fax to EDI	1 2	❒	❒	_____
Binary support (mailbox size limit)	1 2	❒	❒	_____
Help desk	1 2	❒	❒	_____
Mapping services	1 2	❒	❒	_____
Educational services	1 2	❒	❒	_____
Trading partner implementation	1 2	❒	❒	_____
Consulting	1 2	❒	❒	_____
Sell or resell translation software	1 2	❒	❒	_____
Activity log, audit features	1 2	❒	❒	_____
Help				
Available __ hours or from ___ a.m. to ___ p.m.	1 2	❒	❒	_____
Available __ days per week	1 2	❒	❒	_____
Reach knowledgeable person on first call	1 2	❒	❒	_____
Total score				

Appendix B
Example Data Security Plan

The example document appearing on the following pages can be used as a model for your organization's data security plan. The security plan supplements the trading partner agreement that your organization enters into with the grant-making agency.

Example Data Security Plan

This document complements a Trading Partner Agreement (TPA) made by the [**Agency**] (identified as: Agency) and [**Trading Partner**] (identified as: Trading Partner) to establish an electronic data interchange (EDI) relationship.

Purpose. This security plan details the methods for ensuring that the EDI system used for transmitting grants management data satisfies Department of Defense (DoD) and federal government security requirements. It addresses the security issues inherent in the use of computers and telecommunications to accomplish traditional paper-based administrative functions. It describes the security classification of the information the system will process. It also summarizes the system's planned security protection strategy including logical security, physical security, personnel security, procedural security, and other protection measures.

References. Department of Defense Directive 5200.28, *Security Requirements for Automated Information Systems,* provides the guidance for this security plan.

1. System Identification

A. Responsible Organization

Agency is responsible for determining that the overall system is operating at an acceptable level of risk for the classification level of data being processed. However, each individual activity is responsible for developing and maintaining control systems sufficient to meet requirements for protecting programs and data from improper access, loss, alteration, lack of availability, or destruction.

Specific responsibility for the operation of the components of the system is as follows:

- Trading Partner system—Trading Partner
- Trading Partner value-added network (VAN)—Trading Partner is responsible for oversight of the Trading Partner's VAN and ensuring that the VAN provides Agency's as specified
- Agency VAN—Agency is responsible for oversight of the Agency's VAN and ensuring that the VAN provides Agency's as specified
- Agency prototype EDI server—Agency
- Surveillance systems—[other named parties for information copy distribution]

B. System Name

EDI System for Grants Management, consisting of:

- Trading Partner system
- VAN (Trading Partner and Agency)
- Agency prototype EDI server
- Surveillance systems—[party receiving information copies]

C. System category: Major Application

D. System operational status: Under development. Note: The majority of components of this system are already operational as support systems for other operations or applications. The "EDI system" refers to the newly established interconnection of the various systems required to transmit and process grants management EDI data. This security plan focuses on the additional controls specifically required to protect the EDI transactions being processed. The use of EDI technology introduces new threats to these existing systems that can compromise the confidentiality and integrity of data.

E. General Description/Purpose: The EDI system will be used to transmit grants management data via EDI from Trading Partner to Agency. The Trading Partner system will transmit data in an X12-compliant format to the appropriate Agency prototype EDI server using VAN electronic mailboxes. The Trading Partner system will use dial-up modem access to connect to the VAN and send the file to the VAN mailbox of the appropriate EDI server. The Agency prototype EDI server will then use dial-up modem access to connect to the VAN, retrieve the file from the mailbox, translate the data file according to predetermined formats, and use File Transfer Protocol (FTP) to route the translated file to the Agency system through the Federal Data Network or other designated Agency network. The Agency prototype EDI server will have a controlled user account on the Agency system with access to a specially designated EDI area/directory where the file will be sent. Further transfer of the data file between the Agency systems will be accomplished through controlled user accounts on the various systems with EDI-specific access limits.

2. Sensitivity of Information Handled

A. Applicable Laws. All federal information systems must satisfy a variety of laws or regulations that establish specific requirements for confidentiality, integrity, or availability of information processed, handled, or managed by the system. Documents establishing security requirements for the EDI system are listed under References.

B. Information sensitivity. At a minimum, all systems will safeguard the EDI data to the same degree as material marked Business Sensitive (For Official Use Only). The methods for protecting facilities, areas, and devices that either contain or are used to access EDI resources will not differ from those used to safeguard other resources with the same security classification. Additional protection requirements of the EDI system are based on its need for information confidentiality, integrity, availability, authentication, and nonrepudiation.

- **Confidentiality.** The system contains business-sensitive (company-proprietary) information that requires protection from unauthorized disclosure. The Trading Partner considers such information to be privileged or confidential information that is exempt from disclosure under the Freedom of Information Act. Unauthorized disclosure of the cost data could have an adverse impact on the Trading Partner's competitiveness. Other possible impacts of data compromise could include adverse publicity for the Agency and costly litigation both for the Trading Partner and the Agency. Protection requirement for this category is high.

- **Integrity.** The system contains information that must be protected from unauthorized modification, whether intentional or not. The data are used for internal Agency analysis. Unauthorized data modification would produce incorrect analysis. Protection requirement for this category is medium.

- **Availability.** The system contains information that should be available on a timely basis to meet mission requirements of analyzing grants management data in support of various programs. However, timeliness of the data is not mission-critical. In other words, this system does not transmit time-critical data (such as a system for air traffic control or electronic funds transfer). Protection requirement for this category is low.

- **Authentication.** The system contains information received from various Trading Partners on a periodic (such as monthly) basis. It is important to validate that data are received from an authorized Trading Partner representative. Protection requirement for this category is medium.

- **Nonrepudiation.** The data being transmitted represent an item from a specified contract. The Trading Partner is required to submit these data to the Agency; therefore, it is important that the system provide sufficient proof (through audit trails) that the data were sent or received. Protection requirement for this category is medium.

C. Security Mode of Operation. The EDI system will operate in a limited ADP access security mode that requires the implementation of special controls to restrict access to only those individuals who by their job function have a need to access the data.

D. Minimum Trusted Class. The minimum trusted class for the EDI system will be sensitive unclassified.

3. System Security Measures

A. Risk Assessment and Management. Agency will conduct a risk assessment of the EDI system every three years unless a significant change occurs in the system before the end of the three-year period. A risk assessment and management review includes an examination of threats and vulnerabilities that may result in deliberate or inadvertent, unauthorized disclosure or modification of data. By matching system vulnerabilities to known threats, Agency can identify risks for which effective countermeasures need to be established. The purpose of a risk management program is to eliminate or reduce identified risks. Agency will conduct an annual review of any significant changes to the system and items found to be noncompliant in the previous assessment.

B. Applicable Guidance. Applicable guidance for the implementation of security measures for the EDI system is listed under References.

C. Security Control Measures.

1. **Management Controls**

   a. Security responsibility. Agency shall oversee the security of the overall system. However, each trading partner is responsible for the selection, implementation, and maintenance of appropriate security products, tools, tests, and procedures sufficient to meet its requirements for protecting its programs and data from improper access, loss, alteration, or lack of availability.

   b. Personnel Screening. Each trading partner is responsible for limiting access to the EDI system (or system procedures, user IDs, and passwords) to only those individuals with a need for such access.

2. **Development/Implementation Controls**

   a. Security specifications. The EDI system shall comply with federal guidelines for automated information systems as listed under References.

   b. Design review and system tests. Design reviews and system tests shall be conducted before placing the system into operation to ensure the system meets security requirements. Results shall be fully documented and maintained in official records.

   c. System Approval. An approving authority designated by Agency-(to be determined) shall ensure that the system meets all applicable federal poli-

cies, regulations, and standards, and that protection measures appear adequate for the level of data being processed.

3. **Operational Controls**

a. Physical and environmental protection. Each activity shall provide the computers and equipment associated with the EDI system with an appropriate level of physical and environmental security including the following conditions: access to the computer area shall be restricted to authorized employees; computer areas shall have appropriate temperature controls and appropriate fire controls (smoke/heat detectors and fire extinguishers); and computers and peripheral equipment shall have surge suppressers/UPSs.

b. Production, input/output controls, records management. Each trading partner is responsible for providing control over the handling, processing, storage, and disposal of EDI system data, including ensuring proper labeling and destruction of media and hard copy outputs in accordance with the security classification and providing appropriate physical security/access control to media, hard copy outputs, and output devices such as printers.

c. Emergency, backup, and contingency planning. If any component of the EDI system fails, alternate means to transmit or process the EDI data shall be provided. Fallback contingencies may range from a completely manual operation to a degraded automated information system, or some combination of the two. The activity responsible for the operation of each EDI component is responsible for developing operational plans for its system to handle emergency situations, back up the EDI system, and respond to contingencies. This issue will need to be reexamined in the future as users become more dependent on the electronic system and it becomes more difficult to return to the manual, paper-based method of processing.

d. Audit and variance detection. The operating systems for the Agency prototype EDI servers will provide discretionary access control and an audit log of violations of system access controls. In addition, VAN security mechanisms such as status control reports and audit trails shall be used as necessary to track access controls on the VAN.

e. Hardware and system software maintenance controls. The responsible system administrator for each component of the EDI system shall maintain logs of repairs, upgrades, and other changes to the system.

f. Documentation. The responsible system administrator for each EDI component shall maintain system documentation including, as appropriate: documentation supporting system hardware and software; results of tests; standard operating procedures for the EDI system; emergency/contingency

plans; user manuals and procedure documents; backup procedures; copies of system risk analyses; and certification/accreditation documentation.

4. **Security Awareness and Training.** Each trading partner is responsible for ensuring that all employees involved with the management, use, design, development, maintenance, or operation of the EDI system are aware of their security responsibilities and trained to fulfill them. An information security training program shall be established for all personnel having access to EDI information, covering such areas as:

a. Computer Security Basics: An introduction to the basic concepts behind computer security practices and the importance of the need to protect the information from vulnerabilities to known threats.

b. Security Planning and Management: A discussion of risk analysis, the determination of security requirements, and security training necessary to perform the computer security function.

c. Computer Security Policies and Procedures: A look at security practices in the areas of physical, personnel, software, communications, data, and administrative security. Users shall be trained in day-to-day procedures for handling sensitive data/programs, conducting security checks, and maintaining the security and integrity of systems and facilities through the use of access control systems and escort procedures.

d. Contingency Planning: A discussion of all aspects of contingency planning, including emergency response, backup, and recovery plans and identification of the roles and responsibilities of all players involved. Users shall be aware of procedures to use to report and handle security incidents such as bomb threats, riots, disturbances, unauthorized personnel in controlled areas, and computer viruses.

5. **Technical Controls**

a. User identification and authentication

1. Trading Partner shall include in the body of the transaction a discrete reference number (authorization code) and password known only to the sender and receiver. These codes shall equate to specific names uniquely identifying an official having approval authority. Neither participant shall disclose its own authorization codes or passwords nor those of the other to anyone else. The authorization information shall be included in the transaction set in data element ISA01/ISA02, and the password shall be included in data element ISA03/ISA04. Agency shall designate a responsible individual to establish and maintain these codes

and passwords in accordance with federal password management guidelines.

2. Trading Partner, Agency prototype EDI server, and Agency shall restrict access to EDI systems, applications, and data by requiring valid user IDs and passwords.

3. Trading Partner shall establish a special user ID and password to access the VAN. User ID, password, and procedures for accessing the VAN shall be restricted on a "need-to-know" basis.

b. Authorization and access controls. In addition to the controls specified in 5.a, where applicable, the activity shall restrict the authorization to access and/or change EDI system and/or data files. System administrators and users shall be granted access and authorization in accordance with their need to perform required functions. Separation of duties shall be used to the extent feasible to protect the system.

c. Data integrity/validation controls

1. Trading Partner shall have send-only capability; Agency shall have receive-only capability (except for X12 transaction set 997—Functional Acknowledgment).

2. A functional acknowledgment (X12 transaction set 997) shall be sent to the sender to indicate whether the transaction set was accepted or rejected.

3. Internal control mechanisms in the X12 transaction set and EDI translation software shall be utilized (interchange control data, functional group control data, transaction set control data, compliance checking, etc.).

4. Activities shall establish security incident reporting to investigate security incidents and inform management of the results of the investigations.

d. Audit trails and journaling. Activities shall maintain logs to provide confirmation control reporting to originators and recipients, including at a minimum:

1. Trading Partner

a) Date and time the originator prepared and sent transaction set from the internal business application to the EDI network/VAN

b) Date and time the functional acknowledgment was received

2. Agency prototype EDI server

a) Date and time the transaction set was retrieved from the VAN

b) Date and time the transaction set was translated

c) Process control log listing results of translation (errors, number of transactions, etc.)

d) Date and time the functional acknowledgment was sent to Trading Partner

e) Date and time the translated file was forwarded to Agency (and if unable to forward, any process control log listing the errors)

3. Agency—Date and time the translated file was received from the EDI server

In addition, VAN security mechanisms such as status control reports and audit trails shall be used as necessary to track the status of the transaction set on the VAN.

6. **Archiving and Data Retention Responsibility**

As the grants management reporting process transitions from the current paper format to electronic format, archiving and data retention requirements must be reexamined. The federal government is currently determining the data retention period necessary to meet contract retention requirements. The following guidance represents interim policy until a final determination can be made.

Trading Partner: The X12 transaction set data file in its original form shall be maintained until the completion date of the applicable contract. Appropriate methods for maintaining the stored records shall be developed and implemented. Trading Partner shall maintain the integrity and security of the files, regardless of how they are stored, and ensure it can retrieve any archived record. Trading Partner shall also maintain audit trails of all records transferred from one medium to another (e.g., paper to computer disk file).

Agency prototype EDI server: The untranslated X12 transaction set file in its original form and the translated X12 file should be maintained until the prototype EDI server is notified by Agency that the file is no longer required. Appropriate methods for maintaining the stored records shall be developed and

implemented. The Agency prototype EDI server shall maintain the integrity and security of the files, regardless of how they are stored, and ensure it can retrieve any archived record. The Agency prototype EDI server shall also maintain audit trails of all records transferred from one medium to another (e.g., paper to computer disk file).

Agency: The translated X12 file in its original form should be maintained until the completion date of the applicable contract. Appropriate methods for maintaining the stored records shall be developed and implemented. Agency shall maintain the integrity and security of the files, regardless of how they are stored, and ensure it can retrieve any archived record. Agency shall also maintain audit trails of all records transferred from one medium to another (e.g., paper to computer disk file).

4. Additional Comments

Electronic data interchange represents an evolving technology and a new way of doing business. As the technology matures and the use of EDI becomes more prevalent, this security plan will be reviewed and revised to incorporate new requirements and new technologies.

Appendix C
Part 10 of the Federal Implementation Guidelines for EDI

The information presented in this appendix comes directly from the *Federal Implementation Guidelines for Electronic Data Interchange (EDI)* prepared by the Federal Electronic Commerce Acquisition Program Management Office (ECA-PMO).

Only Part 10—Federal Conventions for Using ASC X12 Transaction Sets is provided in this appendix. It includes the instructions for implementing the control and security structures and definitions of the usage indicators and applicable codes. The other parts of the Federal Guidelines are available at the "Secretariat for Federal EDI" Web site maintained by the National Institute of Standards and Technology (NIST).[1]

[1]Secretariat for Federal EDI (Web site), http://snad.ncsl.nist.gov/dartg/ edi/fededi.html.

PART 10—FEDERAL CONVENTIONS FOR USING ASC X12 TRANSACTION SETS

This version of Part 10 of the Federal Implementation Guidelines, based on the ANSI ASC X12 Version 003 Release 070 standards, supersedes and cancels the August 1994 version of Part 10.

Except where specifically otherwise indicated, this document directs how the agencies, components and activities of the United States Federal government will exchange Electronic Data Interchange (EDI) data formatted in accordance with the provisions of the ANSI ASC X12 standards.

10.1 INTRODUCTION

The power of the American National Standards Institute (ANSI) Accredited Standards Committee (ASC) X12 standard is in its building block concept, which standardizes the essential elements of business transactions. The concept is analogous to a "standard bill of materiel and the construction specifications," which gives the architect flexibility in what can be designed with standardized materiel and procedures. The Electronic Data Interchange (EDI) system designer, like the architect, uses the ASC X12 standards to build business transactions that are often different because of their function and yet utilize the ASC X12 standards. The "bill of materiel and the construction specification" of ASC X12 are the standards found in the published technical documentation.

ASC X12.3, December 1996—The *Data Element Dictionary* specifies the data elements used in the construction of the segments that comprise the transaction sets developed by ASC X12.

ASC X12.5, December 1996—The *Interchange Control Structure* provides the interchange control segment (also called an envelope), consisting of a header and trailer, for the EDI transmission; it also provides a structure to acknowledge the receipt and processing of the envelope.

ASC X12.6, December 1996—The *Application Control Structure* defines the basic control structures, syntax rules, and semantics of EDI.

ASC X12.22, December 1996—The *Data Segment Directory* provides the definitions and specifications of the segments used in the construction of transaction sets developed by ASC X12.

ASC X12.58, December 1996—The *Security Structures* define the data formats for authentication, encryption, and assurances in order to provide integrity, confidentiality, verification and non-repudiation of origin for two levels of exchange of

Electronic Data Interchange (EDI) formatted data: functional group and transaction set level.

X12.59, December 1996—The *Implementation of EDI Structure/Semantic Impact* provides a clear distinction between the syntax of X12 structures and the semantics of transaction set usage.

X12C/TG1/95-65—*Technical Report Reference Model for the Acknowledgment and Tracking of EDI Interchanges* summarizes the use of the ANSI ASC X12 control elements and standards for the acknowledgment and tracking of EDI interchanges.

International Telecommunication Union—Telecommunication Standardization Sector (ITU-T) Recommendation X.509 *(1993)/ISO/IEC 9594-8 (1995), Information Technology- Open Systems Interconnection- The Directory: Authentication Framework. The Directory,* defines a framework for the provision of authentication services by the Directory to its users. It specifies the form of authentication information held by the Directory, describes how authentication information may be obtained from the Directory, states the assumptions made about how authentication information is formed and placed in the Directory, defines three ways in which applications may use authentication information to perform authentication, and describes how other security services may be supported by authentication.

In addition to using existing standards to build specific transactions, the standards may be used to provide control and tracking of interchanges if accomplished in a specific standardized approach. ANSI ASC X12 has defined and approved several control structures and Transaction Sets intended to augment EDI auditing and control systems. It is the intent of these standards to provide a tracking mechanism for EDI data as it moves through the transmission cycle. Through the implementation of these tracking tools and analysis of the resulting information, delay or failures in delivery can be identified and corrected.

The work accomplished by ANSI ASC X12C in this area produced a generic acknowledgment model that has been adapted to support Federal Government EDI processes. Implementation of the acknowledgment mechanisms identified by this model will provide a basic capability to track interchanges as they flow from senders through Service Request Handlers (SRH) to receivers across the EC/EDI Infrastructure. (An SRH is a service provider whose primary function is to provide communications services between other components in the model.) This basic capability will provide functionality for each component to determine translation and transmission status, including current location and disposition of an interchange. Use of the implemented acknowledgment mechanisms to determine singular event status can provide components with the information necessary to obtain some level of confidence that interchanges are flowing through the infrastructure properly. Taken as a sequence of acknowledgment events, the model provides senders with

a means to track interchanges from generation to delivery to a Service Request Handler at the boundary of the infrastructure, without imposing the processing and communications overhead that would be required for true application to application acknowledgments.

In addition, the implemented acknowledgment mechanisms of this model will allow individual components to build upon or enhance their internal audit trail processes.

This part of the Federal Implementation Guidelines is meant to be an overarching architecture of the control and security structure which the government is implementing in the Electronic Commerce Infrastructure (ECI) and other government EC activities. However, not all the parts of the architecture will be implemented immediately. The specifics of which parts are actually implemented will be defined in agreements between actual components in the trading network and architecture, such as Value Added Networks (VANs) and government users of the ECI.

It is not the intent of this guideline to specify how the implemented acknowledgment mechanisms are to be used. While support of these mechanisms is required, their usage between infrastructure components will be as agreed between those components. As an example, the use of certain acknowledgment mechanisms between the government and VANs is specified in a VAN Licensing Agreement (VLA). Where there is a conflict between the implementation guidance provided in Part 10 and the VLA, the VLA shall take precedence. Also, the use of acknowledgments between Government Points of Translation (GPoT) and other infrastructure components can be as mutually agreed upon.

The Service Level Agreement (SLA) between the ECI and the respective government Automated Information Systems (AIS) acts in a similar manner as the VLA. Where there is a conflict between the implementation guidance provided in Part 10 and the SLA, the SLA shall take precedence.

By focusing on basic acknowledgment functionality that is independent of communications protocols, enhanced tracking of interchanges is accomplished without requiring individual components to adhere to or support a full accountability system.

For further clarification of acronyms, abbreviations, and codes, refer to ASC X12 published technical documentation. For copies, contact either the EDI focal point within your service or agency, or, alternatively, contact the administering body (see Section 1.3 of these guidelines).

10.2 CONTROL SEGMENTS

In addition to communications control, the EDI interchange structure provides the standards user with multiple levels of control to ensure data integrity. It does so by using header and trailer control segments designed to identify uniquely the start

and end of the interchange functional groups and transaction sets. The relationship of these control segments is shown in Figure 10.2-1. Control Segment specifications are defined in Section 10.6.

10.2.1 DESCRIPTION OF USE

The interchange header and trailer segments (ISA/IEA) along with the optional interchange acknowledgment segments (TA1 and TA3) constitute the interchange control structure (i.e., an interchange envelope). Interchange control segments perform the following functions:

- Define data element separators, subelement separators and data segment terminators
- Provide control information
- Identify interchange sender and receiver
- Allow for authorization and security information.

The actual interchange control structure includes neither the group control structures nor the transaction control structures; these are defined by ASC X12 as application control structures, and their version and release may differ from those for the interchange envelope. An interchange envelope encompasses one or more functional groups (GS/GE), which, in turn, enclose one or more related transaction sets (ST/SE). The relationship for these structures is illustrated in Figure 10.2-1.

The purpose for GS/GE functional grouping is to provide an additional control envelope surrounding like transaction sets conforming with a unique Implementation Convention (IC). Their usage is prescribed as interchange control segments in order to present a consistent methodology for electronic data interchange within the government community and for commercial entities that conduct EDI business with the government.

Implementation Note: *The Federal Government Electronic Commerce Infrastructure (ECI) shall send and receive textual data ASCII encoded. If unencrypted binary segments are filtered, Base 64 filtering shall be used.*

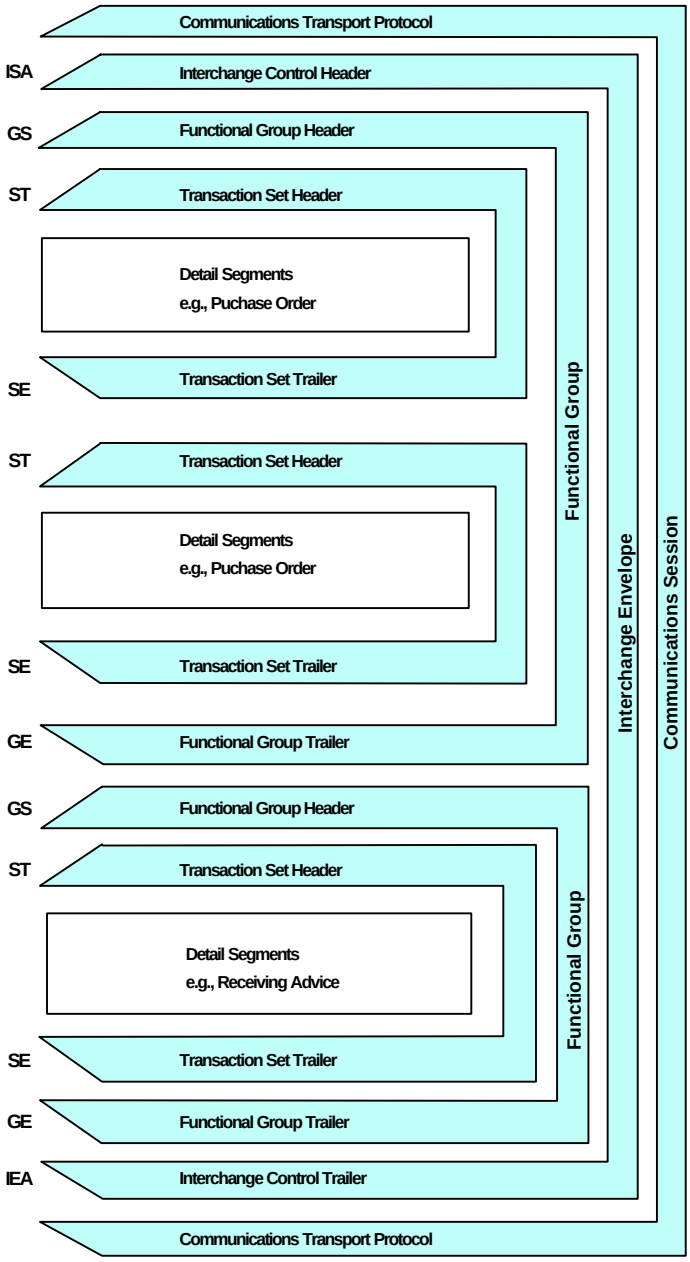


Figure 10.2-1 Hierarchical Structure

Note: When an Interchange contains TA3s, it shall contain only TA3s. The TA3s replace all Functional Groups, Security Envelopes, Transaction Headers and Trailers, as well as Detail Segments in the above diagram.

10.2.1.1 DATA ELEMENT, DATA SEGMENT, AND COMPONENT DATA ELEMENT SEPARATION

In ASC X12 documentation, the data element separator is graphically displayed as an asterisk (*). The actual data element separator employed within the interchange envelope dictates the value for the entire interchange. The first occurrence of the data element separator is at the fourth byte of the interchange control header. The value appearing there dictates the data element separator used through the next interchange trailer.

In a similar manner, the interchange control header establishes the value to be used for segment termination within an interchange. ASC X12 documentation represents this graphically by a new line (N/L). The first instance of segment termination occurs immediately following the ISA16 data element, and the data value occurring there sets the value for the interchange.

Designation of a component data element separator differs from the other separators in that the ISA segment provides a discrete element (ISA16) for defining the component data element separator data value.

***Implementation Note**:*

1. ASCII hexadecimal character 1C shall be used as the segment terminator in Federal Government interchanges.

2. ASCII hexadecimal character 1D shall be used as the data element separator in Federal Government interchanges.

3. ASCII hexadecimal character 1F shall be used as the component element separator in Federal Government interchanges.

4. These characters are reserved for these purposes and shall not be used in data elements, except that they may be used in data element 785, Binary Data.

10.2.1.2 IDENTIFICATION OF IMPLEMENTATION CONVENTION

The Federal Government develops and maintains Implementation Conventions (ICs) based on ASC X12 standards. All entities conducting EDI business within the Government or externally with the Government shall comply with all applicable ICs. ICs are available from National Institute of Standards and Technology acting as the secretariat for the Federal EDI Standards Management Coordinating Committee (FESMCC). Conventions on the use of interchange control structures are provided herein to document a consistent approach to control structure content. The functional group control structures include the ability to identify specific ICs to which the Transaction Sets contained within that group conform. Interchange senders will provide the ASC X12 Version/Release/Subrelease and implementation

convention identifier in GS08. This identifier uniquely identifies the convention to which the transaction set conforms.

Implementation Note: *Envelope control segments have few options and, except for minor tailoring, are identical for every EDI interchange. The tailoring involves the code values selected for the GS01 and GS08 elements. GS01 classifies the particular transaction set(s) within a functional group and GS08 identifies the specific IC with which the transactions contained within the group comply. (Note: The version and release identified in ISA12 pertains to the interchange control envelope, not to the contained transaction sets.)*

The Version/Release/Industry Identifier Code (GS08) is structured as follows:

Positions 1 through 6:	ANSI ASC X12 Version and Release number (e.g. 003010) upon which the IC is based.
Position 7:	Organizational Scope F = Federal D = DOD G = Government (transitional)
Positions 8 through 10:	Transaction Set Identifier Code (e.g. 850).
Position 11:	Derivative: A character used to differentiate between different functional implementations of the same transaction set. If the convention is not a derivative, an underscore (_) will appear in this position.
Position 12:	A sequential number starting with 0 and incremented by 1 each time the convention is re-issued.

An example of the Version/Release/Industry Identifier Code for X12 Version 003050, Federal IC, revision 1, Commercial Invoice (810C) is 003050F810C1.

10.2.1.3 CONTROL NUMBERS

ASC X12 standards provide for syntax control on three levels: interchange, group, and transaction. Within each level, control numbers exhibit a positive match

between the header segment and its corresponding trailer (i.e., ISA/IEA, GS/GE, and ST/SE). Assignment of these control numbers, at each level, is as follows:

Implementation Note: *ISA/IEA Interchange Control Numbers (ISA13/IEA02).*

1. The nine-digit interchange control number is usually assigned by the originator's translation software. Originating organizations may use any numbering scheme consistent with their business practices.

2. The scheme must provide sufficient uniqueness to identify each interchange. Unique identification is defined as the triplet: Interchange Sender ID, (ISA05, ISA06), the Interchange Receiver ID, (ISA07, ISA08) and the nine-digit Interchange Control Number (ISA13). This triplet shall be unique within a reasonably extended time frame.

3. If there is no TA3, Interchange Delivery Notice, after 2 hours, then retransmit with the same interchange control number (ISA13).

4. If an interchange is rejected, the corrected interchange shall have a new interchange control number (ISA13).

Implementation Note: *GS/GE Data Interchange Control Numbers (GS06/GE02).*

1. This is a one to nine-digit number usually assigned by the originator's translation software. This number uniquely identifies functional groups transmitted between sending and receiving application pairs. Originating organizations may use any numbering scheme consistent with their business practices.

2. The scheme must provide sufficient uniqueness to identify each functional group. The Group Control Number value (GS06), together with the Application Sender's Code (GS02), Application Receiver's Code (GS03), and Functional Identifier Code (GS01), shall be unique within an extended time frame—such as a year.

Implementation Note: *ST/SE Transaction Set Control Numbers (ST02/SE02). The originator's translation software usually assigns the transaction set control number. Originating organizations may use any numbering scheme consistent with their business practices. The scheme must provide sufficient uniqueness to identify each transaction set, within the context of the functional group.*

The control numbers within corresponding header and trailer segments must match. This provides a means to detect loss of data.

10.3 ADDRESSING

The purpose of addressing is to provide an unambiguous reference to a transmission's sender and intended receiver. The addressing model used by the Federal Government for ASC X12 EDI transmissions is graphically depicted in Figure 10.3-1. In this model, there is addressing for two types of transmissions. The first is an interchange. It consists of control segments and application data. The second type is application data. Application data flow from the sending to the receiving applications and is transported within an interchange. Since interchanges are assembled by the sending translation point and disassembled by the receiving translation point, the flow of an interchange is defined to be from translation point to translation point. Application data must be provided to the sending translation point by the sending application and is depicted as a User Defined File (UDF). It must also be provided to the receiving application by the receiving translation point and is also depicted as a UDF.

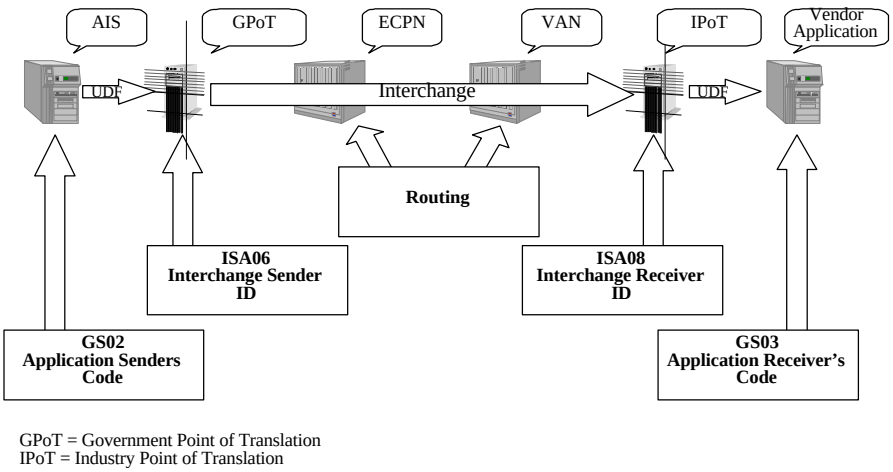


Figure 10.3-1 Addressing Model

While the model depicts data flow from the government to a vendor, it is equally applicable in the reverse flow.

10.3.1 INTERCHANGES

Interchanges flow between translation locations. The Government Point of Translation (GPoT) can be implemented as part of the government Application Information System (AIS), as part of the Electronic Commerce Processing Node (ECPN), or as a stand-alone function. Likewise, the Industry Point of Translation (IPoT) on the vendor side can be in the Vendor Application, as part of the VAN's services, or as a stand-alone function.

The GPoT and IPoT are addressed by the Interchange Sender ID (ISA05 and ISA06) and Interchange Receiver ID (ISA07 and ISA08) data elements. These, combined with the Interchange Control Number (ISA13), create a triplet that defines a globally unique identifier for the interchange. The ASC X12 Interchange flows between these translation points.

Implementation Note:

1. When an interchange contains one-to-one transactions, the Interchange Sender ID (ISA06) and Interchange Receiver ID (ISA08) data elements shall be the addresses of the interchange translation points (both government and non-government).

2. Translation Points (ISA06 and ISA08) shall be identified via a unique identifier from one of the sources listed as allowable codes in the ISA05 definition in section 10.6. The Data Universal Numbering System (D-U-N-S) number and D-U-N-S +4 are the preferred identifiers.

3. All commercial and government entities conducting business electronically shall provide their translation point (ISA06/ISA08) codes during registration.

4. In the ECI, when an interchange contains public transactions the ISA08 will be addressed individually to all certified VANs, not necessarily each IPoT. The ISA06 will contain the ECPN's address.

10.3.2 APPLICATION SENDER AND RECEIVER CODES

Application data is transported within the interchange via groups. Group addressing (GS02/GS03) must define the user application end points shown in figure 10.3-1 as the AIS and the Vendor Application. These addresses are locally unique and are defined between the translation point and its customers. The data that flows between the translation points and the Application Senders and Receivers are not defined by ASC X12, but are in a format agreed between the applications and their translation points.

ASC X12 standards provide for the identification of senders and receivers on two levels, the interchange and the group. The group level identifies application senders and receivers. Depending on where translation is performed, the sender/receiver IDs may be the same at the interchange and group levels and may use any number of available naming schemes.

At the GS/GE level, D-U-N-S and D-U-N-S plus 4 are recommended, especially for identifying government organizations. Other identifiers may be used.

A D-U-N-S number may be acquired from Dun and Bradstreet and the plus 4 portion of the number is assigned and maintained internally by each entity. Specific use of these numbers is provided for in the control structures section of this document.

Implementation Note:

1. The GS02/03 identifiers need be unique only within the context of the associated ISA address.

2. All commercial and government entities conducting business electronically shall provide their Application Sender and Receiver (GS02/GS03) codes during registration.

10.4 ACKNOWLEDGMENTS

The successful conduct of business via EDI requires that trading partners be able to determine when transactions were received, not received, received in error, or otherwise did not complete the transmission or receiver application processing cycle. The generation or handling of these events may be communications based, EDI processing based, or both. In addition, senders may desire to know such information on an exception basis, such as reporting only for error conditions, or they may need regular indication of the status of delivery to allow them to maintain local, internal audit information. Also, providers of communications services may need to know when interchanges for which they have accepted responsibility were forwarded and accepted by the next service provider in the transmission path, or whether forwarding was not successful.

In either scenario, the transmission or processing of interchanges can be viewed as an acknowledgment event in a general sense, creating the need for some response. From a sender's perspective, the acceptance of their interchange by a translator or communications provider is an acknowledgment event that could either be indicated by a simple receipt, or a more thorough reporting of what actions were taken after receipt. For a service provider, forwarding interchanges can also result in an acknowledgment event being created that calls for an acknowledgment action to take place.

Taken as a set of acknowledgment requirements, these and other events can be considered as a set of circumstances which results in or require some acknowledgment action to take place. Rather than consider every possible action and event, a basic sub-set of these events can be defined that describes the majority of cases that form a generalized picture of tracking interchanges. Together with acknowledgment mechanisms that relate to those events and specific components that create or respond to those events, an acknowledgment model can be described.

ANSI ASC X12C has worked in this area, having produced a generic Acknowledgments Model in X12C/TG1/95-65—*Technical Report Reference Model for the Acknowledgment and Tracking of EDI Interchanges*. This technical report identifies specific entities in the EDI communications and processing path that serve as the event generators or handlers, as well as identifying X12 standards based ac-

knowledgment mechanisms. Also, the senders and receivers of the interchanges are recognized as being the terminating application systems for which the EDI transactions are sent from or sent to, regardless of where translation occurs. The government has taken the ANSI X12 approach to an acknowledgments model, refining it through identification of specific entities and acknowledgment events. Support for this model will provide users and service providers with the ability to track interchanges and respond to requests for status of such interchanges. In addition, the internal audit trail processes of each entity will be enhanced with the availability of specified event mapping.

10.4.1 DESCRIPTION OF ACKNOWLEDGMENT MODEL

As adapted from the generic model developed within ASC X12C, the Government Acknowledgment Model identifies specific components, acknowledgment events, and X12 mechanisms that are related to those events. Based upon the Electronic Commerce Processing Node (ECPN) as a central component, the model establishes a view of the EC/EDI Infrastructure as encompassing commercial and government entities, as well as service providers and users.

In this model, service providers are those components that provide translation services, communications services, or some EDI processing services. Specifically, the model identifies the ECPNs, VANs and Translation Points as service providers. A Service Request Handler (SRH) is a service provider whose primary function is to provide communications services between other components in the model. Users include Trading Partners (TPs) and Automated Information Systems (AISs).

The acknowledgment mechanisms identified in the model include unspecified as well as X12 based mechanisms. Where the model has identified an acknowledgment event but does not specify a mechanism for handling that event, it is implied that components involved in that event will agree on what mechanism will be used.

X12 based acknowledgment mechanisms include control segment structures in addition to transaction sets. The Interchange Delivery Notice (TA3) segment, Data Status Tracking (242) transaction set and the Functional Acknowledgment (997) transaction set all have distinct properties and functions. However, their use in a general sense as acknowledgment mechanisms allows a sequence of communications and processing events to be tied together in a logical stream. Each acknowledgment event is mapped to an X12 standards based mechanism according to where the event takes place, what type of event occurred, and what role the receiving or generating component plays in the data flow stream.

The TA3 can provide information on the status of delivery of an interchange, the time an interchange was received, or the disposition of an interchange, and is used to report such information between Service Request Handlers. The Data Status Tracking (242) transaction set, in addition to providing the ability to represent the information contained in the TA3, allows transmission status information to be

conveyed from service request handlers to senders. The Functional Acknowledgment (997) transaction set indicates the status of translation of the interchange header and trailer information. These mechanisms are more fully described later in this section.

The model, as depicted in Figures 10.4-1, 10.4-2, 10.4-3, and 10.4-4, identifies the sets of events that, through implementation and use of the specified acknowledgment mechanisms, provides for the tracking of interchanges across the infrastructure.

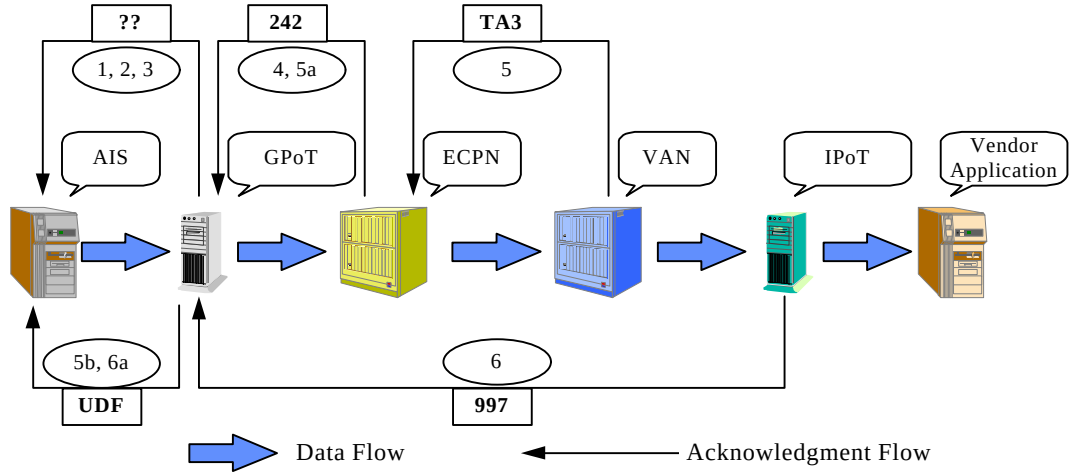
Implementation Note:

1. While the requirement for acknowledgments from Government Points of Translation (GPoT) *to supported AISs was identified, no single mechanism could be identified. It is therefore left to agreement between them as described in the Service Level Agreement.*

2. TA1 is not supported in this acknowledgment model implementation.

3. The government translation function can be implemented as part of the government Application Information System (AIS), as part of the Electronic Commerce Processing Node (ECPN), or as a stand-alone function. GPoT acknowledgment responsibilities reside at the location performing translation.

The vendor translation function can be implemented as part of the Vendor Application, Value Added Network (VAN) or as a stand-alone function. IPoT acknowledgment responsibilities reside at the location performing translation.



Notes:
a. The GPoT translation function may be performed by the ECPN, AIS, or by a separate entity.
b. For the purposes of the model, the govt-to-govt scenario is represented by replacing the VAN-Translation components with a GPoT component.
c. The IPoT may be operated by the VAN, the Vendor, or a third party. In all cases, the IPoT is the ultimate recipient of the interchange for the purposes of acknowledgment in this model.
d. 997s and 242s can be mapped at the GPoT to UDFs & forwarded to the AIS as agreed between the GPoT and their customer base. 242s will not be acknowledged by 997s.
e. UDF is User Defined File (flat file, proprietary file).
f. The use of 824s are not precluded by this model.
g. Support for the model acknowledgment mechanisms is mandatory. The manner of their usage is as detailed further in the Federal EDI Implementation Guidelines Part 10, or other agreements.

Figure 10.4-1 Acknowledgment Model, Commercial to Government

Sequence/Event	Mechanism	From	To
1. Receipt of UDF by GpoT	TBD	GPoT	AIS
2. Translation Result	TBD	GPoT	AIS
3. Disposition (Acknowledge that interchange has left GPoT)	TBD	GPoT	AIS
4. Interchange receipt by ECPN	242	ECPN	GPoT
5. Interchange Disposition at SRH	TA3	VAN	ECPN
(Government to Government)	TA3	GPoT	ECPN
5a Report of Interchange Disposition at SRH	242	ECPN	GPoT
5b. Report of Interchange Disposition at SRH	UDF	GPoT	AIS
6. Translation Result	997	IPoT	GPoT
6a Translation Result	UDF	GPoT	AIS

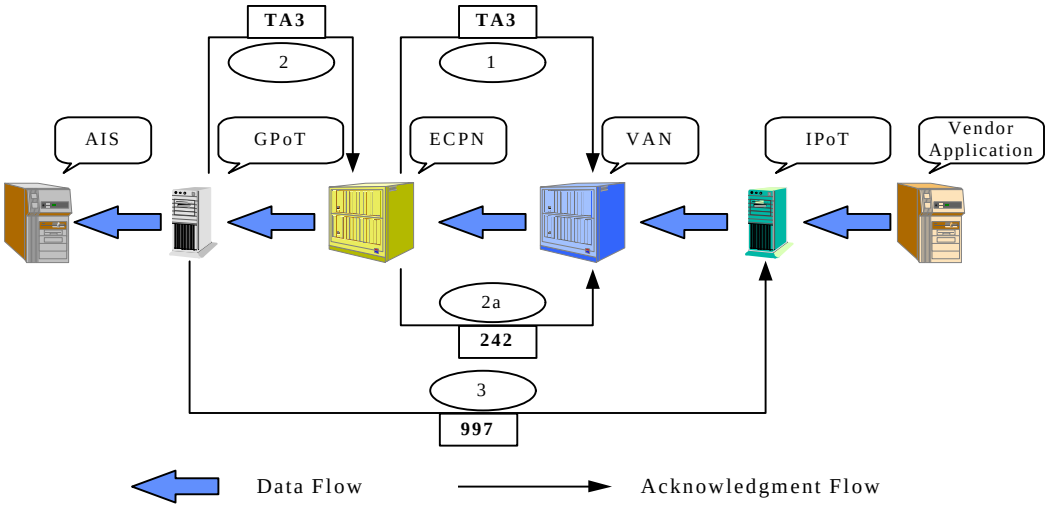
Notes:

Not all events 1, 2 or 3 may occur or need to be acknowledged

TBD indicates the acknowledgment mechanism is to be determined, or as agreed to between components

UDF: User Defined File (flat file, proprietary file format)

Figure 10.4-2 Acknowledged Events, Commercial to Government



Notes:
a. Acknowledgments among VANs, Translation Points and their customers are matters to be decided by them and are not defined in the government Acknowledgment Model.
b. Some GPoTs may generate a second 242, with the ECPN acting as a pass-through.
c. For government to government scenario, replace the VAN with a GPoT. The ECPN will generate 242s in lieu of TA3s in step 1.

Figure 10.4-3 Acknowledgment Model, Government to Commercial

Sequence/Event	**Mechanism**	**From**	**To**
1. Interchange receipt by ECPN (Government to Government)	TA3 TA3	ECPN ECPN	VAN GPoT
2. Interchange Disposition at GpoT	TA3	GPoT	ECPN
2a. Report of Interchange Disposition at GPoT (Government to Government)	242 242	ECPN ECPN	VAN GPoT
3. Translation Result	997	GPoT	IPoT

Note: In step 2a, the disposition report carried in a TA3 is mapped to a 242.

Figure 10.4-4 Acknowledged Events, Government to Commercial

10.4.2 INTERCHANGE ACKNOWLEDGMENT

At the interchange level, acknowledgments can occur for a number of events. Successful translation, syntax error, or a more detailed acknowledgment of the disposition of an interchange can be reported. The available X12 mechanisms for such interchange acknowledgments includes the Functional Acknowledgment (997) transaction set, the Interchange Acknowledgment (TA1), and the Interchange Delivery Notice Segment (TA3). In general, the 997 is used exclusively for reporting the status of syntactical analysis of the interchange by the receiving translator, although it could be used as an indication that an interchange was received. The Interchange Acknowledgment (TA1) is not supported in this acknowledgment model. The Interchange Delivery Notice (TA3) provides the ability for reporting on the status of actions taken on a particular interchange. The manner in which these mechanisms are used, and the features within each that are utilized, provides a set of tools for building a sequence of acknowledgments for the life cycle of an interchange as it flows across an infrastructure.

10.4.2.1 TA3

The purpose of the TA3 is to provide a notice from the receiving SRH to the sending SRH that an interchange was delivered, not delivered, refused, purged, or transferred to the next SRH. It provides a notification of action taken, notice of time/date action was taken, and the ability to report on more than one event.

As an acknowledgment mechanism in this model, the TA3 is used between the ECPN and VANs, as Service Request Handlers, to indicate the status of interchanges sent from the government to commercial components, as well as the reverse scenario. To indicate outbound delivery status, the information contained in this TA3 is further translated into a 242 transaction set and sent to GPoTs for their use, which may include supplying this information to the interchange sender. The government uses the TA3 to indicate interchange delivery status to the sending commercial infrastructure components.

Implementation Note:

1. An interchange that contains a TA3 shall contain only TA3s.

2. An interchange may contain multiple TA3s.

3. Upon delivery to the interchange receiver's mailbox, a TA3 shall be generated.

4. If delivery to the interchange receiver's mailbox is not made within 2 hours, a TA3 shall be generated indicating a non-delivery status. The appropriate reason codes will be specified. A TA3 shall be generated every 2 hours indicating non-delivery status until the interchange is delivered to the receiver's mailbox. Upon delivery, note 3 above applies.

5. If an interchange is accepted but subsequently determined to be non-deliverable, a TA3 shall be generated indicating code RJ in TA312 and the appropriate reason code in TA303.

6. No acknowledgment is made for the receipt of a TA3.

10.4.2.2 Data Status Tracking (242) Transaction Set

The Data Status Tracking (242) transaction set conveys status information from a service request handler to the interchange sender, interchange receiver, or both. It can be used to provide status information regarding an interchange as it flows from an interchange sender through one or more service request handlers to an interchange receiver during its transmission cycle.

In the acknowledgment model, the 242 transaction set is used for two events: (1) it conveys information from the TA3 that was generated by the VAN or GPoT that received the interchange, and (2) it is used to provide acknowledgment information between government components. Because it is a transaction set, translation sites can map that information into a UDF for the sending applications use. How this information is used depends on the internal business processes at the application site, and is not covered by the model. In addition, this information may be used by the GPoT in its capacity as a Service Request Handler for internal audit trail purposes.

***Implementation Note**:*

1. For interchanges between government components, a 242 shall be generated upon delivery to the interchange receiver's mailbox. If delivery to the interchange receiver's mailbox is not made within 2 hours, a 242 shall be generated indicating a non-delivery status.

2. The 242 transaction set shall not be acknowledged (via a 997), nor shall it be used to report the final disposition of a 997 transaction set.

3. Additional 242 acknowledgments from interconnect service providers may be required by additional agreements among trading partners.

10.4.2.3 Interchange Acknowledgment Segment (TA1)

The Interchange Acknowledgment Segment (TA1) is used to acknowledge receipt of one interchange header and trailer envelope.

***Implementation Note:** The TA1 is not supported in this acknowledgment model.*

10.4.3 APPLICATION ADVICE (824) TRANSACTION SET

Although it can provide acknowledgment functionality, use of the Application Advice (824) transaction set is not specified by this model. Currently, it is primarily used on an exception basis for reporting between applications, and its full use as an acknowledgment mechanism within the model would create substantial impact on the communications and processing systems.

10.4.4 FUNCTIONAL ACKNOWLEDGMENTS (997) TRANSACTION SET

While the Functional Acknowledgment (997) transaction set is not part of the interchange control structure, it is integral to the overall process for interchange integrity, and for completeness of the acknowledgment model.

Support for the Functional Acknowledgment is required in all cases. The 997 verifies (or challenges) the syntactical correctness (e.g., ability to translate) of transaction-level data within a functional group.

***Implementation Note**:*

1) Syntactic correctness shall be determined by comparison to the requirements of the applicable implementation convention, not simply the ASC X12 standard.

The 997 transaction set shall not be acknowledged.

When an X12 transaction containing "Not Used" segments and/or data elements is received by the Government, the transaction will be rejected and a 997 will be generated indicating why the transaction was rejected.

10.5 SECURITY

ASC X12.58, published in December, 1996, provides for the implementation of security services at the functional group and transaction set levels. The available security services include: data integrity, confidentiality, assurance, verification, and non-repudiation of origin. These services may be implemented individually or in any combination.

ASC X12.58 can meet several security objectives. Among these are:

The recipient of an EDI transaction can verify the identity of the originator of the transaction.

The recipient of an EDI transaction can verify the integrity of its contents.

The originator of an EDI transaction can provide confidentiality for its contents.

ASC X12.58 provides a mechanism that can be applied to the X12 functional group or transaction set, in contrast to other alternatives which are usually applied to the entire interchange. ANSI X12.58 is transaction data independent. When X12.58 security mechanisms are applied inside the interchange, they can be handled and routed as standard X12 transactions without disrupting the end-to-end security. Since security services are applied within the interchange, they are independent of the mechanism used to transport them. Thus X12.58 can provide security even when the interchanges leave the boundaries of the ECI.

The Federal Government is committed to providing security services for ASC X12 compliant EDI via the constructs provided by ASC X12.58. However, very significant changes to those constructs have been made within various version/releases of the ASC X12 standards. Also, ASC X12.58 security constructs are not backward compatible. That is, 003070 constructs may not be applied to provide security services to the bulk of the current federal implementations, which are in version/release 3060, 003050, 3040 and earlier.

10.5.1 AUTHENTICATION

- Message authentication is a procedure to verify that received messages have not been alter
  hash function, a public function that maps a message of any length into a fixed hash value,
  used as an authenticator when used in conjunction with some form of data encryption, such
  digital signature.

Implementation Note: *Assurance via the S2A/SVA segments shall be used in lieu of authentic*

10.5.2 CONFIDENTIALITY (ENCRYPTION)

The X12.58 standards allows for the implementation of various algorithms to encrypt X12 transactions. Cryptographic algorithms fall into two categories: secret key and public-key. Secret key algorithms are based on both the sender and receiver sharing the same secret key (i.e., key unknown to other parties). This key is used to encrypt the transaction prior to transmission and decrypt it upon receipt. Public-key algorithms are based on both sender and receiver having a pair of keys, one public and one private. All exchanges of keys between sender and receiver are limited to the public portion only, so the private key portion is protected. Initially, the Government will support the following encryption algorithms:

- Data Encryption Standard (DES)
- Triple DES (DE3)
- Rivest-Shamir-Adleman (RSA)
- SKIPJACK

Implementation Note:

1. Confidentiality services may be applied at either the functional group (GS/GE) level, the transaction set (ST/SE) level or both.

2. When applied, the S1S shall be inserted immediately after the GS segment and the S1E shall be inserted immediately prior to the GE segment

3. When applied, the S2S shall be inserted immediately after the ST segment and the S2E shall be inserted immediately prior to the SE segment.

10.5.3 ASSURANCE (DIGITAL SIGNATURES)

A digital signature is an authentication technique that also includes measures to counter repudiation by the source. Assurances (S1A or S2A and SVA), as defined in X12.58, allow the originator of the transaction to express "business intent" via a digital signature. The Government will support implementation of the Digital Signature Standard. When used, one S2A and one SVA are inserted immediately before the SE segment of the transaction set being assured. If subsequent assurances are applied, additional S2A/SVA pairs are inserted between the previous assurance, and the SE segment of the transaction set being assured. Detailed instructions for the use of the S2A and SVA segments are contained in section 10.6

Implementation Note:

1. Assurance (digital signature) may be applied at either the functional group (GS/GE) level, the transaction set (ST/SE) level or both.

2. When digital signature is applied at the group level, the S1A and SVA segment pair(s) shall be inserted immediately preceding the GE segment of the group being assured (digitally signed).

3. When digital signature is applied at the transaction set level, the S1A and SVA segment pair(s) shall be inserted immediately preceding the SE segment of the transaction set being assured (digitally signed).

When both assurance and confidentiality are applied, assurance (S1A or S2A and SVA) shall be applied first and then confidentiality (S1S and S1E or S2S and S2E).

10.5.4 X12.58 CAPABILITIES BY RELEASE

ANSI X12 Release	**Authentication**	**Encryption**	**Assurance**
3040	(Note 1)	(Note 3)	
3050	(Note 1)	(Note 3)	
3060	(Note 2)	X	X
3070	(Note 2)	(Note 3)	X

NOTES:

1.Authentication accomplished using a message authentication code (MAC). The MAC is a hash of the data.

2.Authentication accomplished as a by-product of the digital signature or by using the MAC defined in earlier releases of the ANSI X12 standard.

3.Private (symmetric) keys supported by this release. Asymmetric keying is possible but not without some “non-standard” use of data elements.

10.5.5 SEQUENCING OF CRYPTOGRAPHIC TECHNIQUES

In practical situations, the users of the X12.58 standards will choose combinations of features rather than just a single feature. This is possible since all features are designed to be used in isolation or in any combination.

Authentication does not protect the confidentiality of the message because the information is interchanged in its plain text form. Message encryption can be used to provide confidentiality while using authentication to provide integrity protection of the same data. When both authentication and encryption are used, the authentication is performed before encryption of the original plain text data.

Where more than one service is selected at a specific level, the order of processing is:

Before applying any security services, the data must first be translated into an EDI format

Addition of one or more assurances

Authentication

Compression

Encryption

Filtering for data communications

When assurance segments are used, they must be added to unsecured (not authenticated or encrypted) transactions. If a transaction set is received (with or without assurances) with encryption and/or authentication applied by the originator, the transaction set must be either decrypted or authenticated prior to the addition of any further assurances. Once any assurances have been added, the transaction set can be encrypted or authenticated prior to being forwarded to additional parties.

When applying security services at the functional group level, all security services at the transaction set level must be completed before applying security services at the functional group level.

The receiving organization processes the received message in the reverse order, starting with inverse filtering, followed by decryption, and then by decompression, validation of authentication and validation of the assurances. When processing inbound security services at the transaction set level, all security services at the functional group level must be removed before processing inbound security services at the transaction set level. In this manner the receiving organization unwraps the EDI message by processing the security services and removing the security segment pairs from the message before processing the next security service.

10.5.6 TRANSMISSION OF SECURITY SEGMENTS

Security services (authentication, encryption and assurances) are provided at two levels within ASC X12 in conjunction with the following envelopes:

- Functional Group (GS/GE envelope)
- Transaction Set (ST/SE envelope)

At each of these levels, authentication, encryption and assurances are each optional. Assurances are independent of authentication or encryption. In addition, any service used at one level is independent of a service used at the other level.

If encryption and/or authentication is provided, the security header segment (S1S or S2S) immediately follows the segment initiating the beginning of this level (GS or ST); the security trailer segment (S1E or S2E) precedes the segment terminating the level (GE or SE). If assurances are present, the S1A or S2A segments and its trailing SVA segment immediately precedes the SE or GE if authentication and/or encryption is not used and immediately proceed the S1E or S2E segment if authentication and/or encryption is used. If encryption and/or authentication at

both levels is provided and if assurances are used at both levels, the sequence of segments, illustrating these levels, is:

ISA-Interchange Header

(Other Groups whether secured or not at Level 1)

GS-Functional Group Header

S1S-Security Header Level 1

(Other Transaction Sets whether secured or not at Level 2)

ST—Transaction Set Header

S2S-Security Header Level 2

(The Transaction Set Segments)

S2A—Security Assurance Level 2

SVA—Assurance Token Level 2

(Other optional S2A-SVA pairs at Level 2

S2E-Security Trailer Level 2

SE-Transaction Set Trailer

(Other Transaction Sets whether secured or not at Level 2)

S1A—Assurance Segment Level 1

SVA—Assurance Token Level 1

(Other optional S1A-SVA pairs at Level 1)

S1E-Security Trailer Level 1

GE-Functional Group Trailer

(Other Functional Groups whether secured or not at Level 1)

IEA-Interchange Trailer10.6 Interchange Control, Acknowledgment and Security Segment Specifications

This section contains the implementation conventions for the:

- Interchange Control Header (ISA), Version/release 003070

- Interchange Delivery Notice Segment (TA3)
- Functional Group Header (GS), Version/release 002003
- Functional Group Header (GS), Version/release 003010
- Functional Group Header (GS), Version/releases 003040 through 003070
- Security Header Level 1 (S1S), Version/releases 003040 and 003050
- Security Header Level 1 (S1S), Version/releases 003060 and 003070
- Security Header Level 2 (S2S), Version/releases 003040 and 003050
- Security Header Level 2 (S2S), Version/releases 003060 and 003070
- Security Assurance Level 2 (S2A), Version/releases 003060 and 003070
- Assurance Token Level 2 (S2A), Version/releases 003060 and 003070
- Security Trailer Level 2 (S2E), Version/releases 003060 and 003070
- Assurance Segment Level 1 (S1A), Version/releases 003060 and 003070
- Assurance Token Level 1 (SVA), Version/releases 003060 and 003070
- Security Trailer Level 1 (S1E), Version/releases 003060 and 003070
- Functional Group Trailer (GE),
- Interchange Control Trailer (IEA), Version/release 003070

Segment: **ISA** **Interchange Control Header**

Usage: Optional

Max Use: 1

Purpose: To start and identify an interchange of zero or more functional groups and interchange-related control segments

Syntax Notes:

Semantic Notes:

Comments:

Notes: ***1. Use ASCII Hexadecimal 1D in the fourth byte of the Interchange Control Header. This first occurrence of an element separator dictates the value the translation software will employ throughout the interchange.***

2. Use ASCII Hexadecimal 1C after ISA16. This first occurrence of a segment terminator dictates the value the translation software employs throughout the interchange.

3. See ISA16 for subelement separator usage.

Data Element Summary

	Ref. Des.	Data Element	Name	Attributes
Must Use	**ISA01**	**I01**	**Authorization Information Qualifier** Code to identify the type of information in the Authorization Information 00 No Authorization Information Present (No Meaningful Information in I02) 05 Department of Defense (DoD) Communication Identifier ***Use to indicate the Department of Defense (DOD) as the information authorizer. Use***	**M ID 2/2**

this code even if the sender is not a DOD entity.

06 United States Federal Government Communication Identifier

Use to indicate the Federal Government as the information authorizer. Use this code even if the sender is not a Federal Government entity.

Must Use ISA02 I02 Authorization Information M AN 10/10

Information used for additional identification or authorization of the interchange sender or the data in the interchange; the type of information is set by the Authorization Information Qualifier (I01)

1. Use to provide additional identification or authorization for the data in the interchange. Otherwise, fill this field with blank characters.

2. When used, it is recommended that the specific coding be exchanged between trading partner data security officials to ensure preservation of data security.

Must Use ISA03 I03 Security Information Qualifier M ID 2/2

Code to identify the type of information in the Security Information

00 No Security Information Present (No Meaningful Information in I04)

01 Password

Use based on trading partner agreement.

Must Use ISA04 I04 Security Information M AN 10/10

This is used for identifying the security information about the interchange sender or the data in the interchange; the type of information is set by the Security Information Qualifier (I03)

If ISA03 is code 00, fill this field with blank characters. Oth-

erwise, enter a password as agreed between Trading Partners.

Must Use ISA05 I05 Interchange ID Qualifier M ID 2/2

Qualifier to designate the system/method of code structure used to designate the sender or receiver ID element being qualified

D-U-N-S (Code 01) or D-U-N-S+4 (Code 16) are prefered.

01	Duns (Dun & Bradstreet)
02	SCAC (Standard Carrier Alpha Code)
04	IATA (International Air Transport Association)
08	UCC EDI Communications ID (Comm ID)
09	X.121 (CCITT)
10	Department of Defense (DoD) Activity Address Code
16	Duns Number With 4-Character Suffix

Must Use ISA06 I06 Interchange Sender ID M AN 15/15

Identification code published by the sender for other parties to use as the receiver ID to route data to them; the sender always codes this value in the sender ID element

1. Enter the identifier of the sender's translation point.

2. 2. Left justify and pad on the right with blanks.

Must Use ISA07 I05 Interchange ID Qualifier M ID 2/2

Qualifier to designate the system/method of code structure used to designate the sender or receiver ID element being qualified

D-U-N-S (Code 01) or D-U-N-S+4 (Code 16) are prefered.

01	Duns (Dun & Bradstreet)
02	SCAC (Standard Carrier Alpha Code)

04	IATA (International Air Transport Association)
08	UCC EDI Communications ID (Comm ID)
09	X.121 (CCITT)
10	Department of Defense (DoD) Activity Address Code
16	Duns Number With 4-Character Suffix

Must Use ISA08 I07 Interchange Receiver ID M AN 15/15

Identification code published by the receiver of the data; When sending, it is used by the sender as their sending ID, thus other parties sending to them will use this as a receiving ID to route data to them

1. Enter the identifier of the receiver's translation point (both government and non-government).

2. Left justify and pad on the right with blanks.

Must Use ISA09 I08 Interchange Date M DT 6/6

Date of the interchange

1. Express the UTC (previously known as GMT) date that this interchange was created.

2. Express the date in a six-position (YYMMDD) format.

Must Use ISA10 I09 Interchange Time M TM 4/4

Time of the interchange

1. Express the UTC (previously known as GMT) time that this interchange was created.

2. Express the time in a four-position (HHMM) format.

Must Use ISA11 I10 Interchange Control Standards Identifier M ID 1/1

Code to identify the agency responsible for the control standard used by the message that is enclosed by the interchange header and trailer

U U.S. EDI Community of ASC X12, TDCC, and UCS

Must Use ISA12 I11 Interchange Control Version Number M ID 5/5

This version number covers the interchange control segments

Use to identify the ASC X12 version and release for the interchange envelope, not the transactions carried within the envelope.

00307 Draft Standards for Trial Use Approved for Publication by ASC X12 Procedures Review Board through October 1996

Must Use ISA13 I12 Interchange Control Number M N0 9/9

A control number assigned by the interchange sender

Originating activities may use any numbering scheme consistent with their business practices. However, the scheme must uniquely identify each interchange over a very long period of time.

Must Use ISA14 I13 Acknowledgment Requested M ID 1/1

Code sent by the sender to request an interchange acknowledgment (TA1)

This request for acknowledgment applies only to return of a TA1, Interchange Acknowledgment. It does not apply to other acknowledgments (e.g. TA3 or transaction set 242) as required by Part 10 of the Federal Guidelines. Since the TA1 is not supported, no acknowledgment shall be requested.

0 No Acknowledgment Requested

Use this code to indicate an interchange acknowledgment via TA1 shall not be returned by the interchange receiver.

Must Use ISA15 I14 Test Indicator M ID 1/1

Code to indicate whether data enclosed by this interchange envelope is test or production

P Production Data

Use to identify all data other than test data.

T Test Data

Use when testing interchanges.

Must Use ISA16 I15 Component Element Separator M AN 1/1

Type is not applicable; the component element separator is a delimiter and not a data element; this field provides the delimiter used to separate component data elements within a composite data structure; this value must be different than the data element separator and the segment terminator

Enter ASCII Hexadecimal 1F. The value of this element dictates the value the translation software employs for component element separation throughout the interchange.

Segment: **TA3** **Interchange Delivery Notice Segment**

Usage: Optional

Max Use: 1

Purpose: To provide a notice from the receiving service request handler to the sending service request handler that an interchange was delivered or not delivered to the interchange receiver's mailbox, or some other ancillary service was performed, and that the interchange receiver retrieved, refused, or purged the interchange; TA3 is exchanged only between service request handlers; use of the TA3 segment is optional

Syntax Notes:

1 If either TA322 or TA323 is present, then the other is required.

2 If either TA324 or TA325 is present, then the other is required.

3 If either TA326 or TA327 is present, then the other is required.

Semantic Notes:

1 TA301 and TA302 identify the service request handlers processing the interchange being reported.

2 TA304 through TA311 and TA318 through TA321 are used to identify the interchange whose status is being reported.

3 TA312 through TA314 identify the action being reported and the date and time that action was performed. TA315 through TA317 provide a second set of interchange action code, date and time that can be included if a given TA3 is reporting on more than one event.

4 TA322 through TA327 contain optional information exchanged by service request handlers to supply additional information concerning actions taken upon the interchange being reported.

Comments:

Notes:

1. Only one interchange action may be reported per TA3. If multiple events are to be reported, multiple TA3s must be used.

2. Only one interchange control structure error may be reported per TA3. If multiple errors are to be reported, multiple TA3s must be used.

Data Element Summary

	Ref. Des.	Data Element	Name	Attributes
Must Use	**TA301**	**I38**	**Service Request Handler ID Qualifier**	**M ID 2/2**
			This is a code identifying the service request handler	
			Cite the code FG to indicate the Federal Government. Do so whether the originator is a public or private organization.	
Must Use	**TA302**	**I39**	**Service Request Handler ID**	**M AN 1/15**
			This is the identification code of the sending service request handler	
			Cite the D-U-N-S or D-U-N-S+4 of the service request handler providing this notice of interchange delivery.	
Must Use	**TA303**	**I43**	**Error Reason Code**	**M ID 3/3**
			The code indicates the error found or not found in processing the control structure or in delivery	

000	No Errors
001	The Interchange Control Number in the Header and Trailer Do not Match; the Value from the Header is used in the Acknowledgment
002	This Standard as Noted in the Control Standards Identifier is not Supported
003	This Version of the Controls is not Supported
004	The Segment Terminator is Invalid
005	Invalid Value as Shown in the Reported Interchange Control Number
006	Invalid Value as Shown in the Reported Interchange Date

007	Invalid Value as Shown in the Reported Interchange Time
008	Invalid Value as Shown in the Reported Interchange Sender ID Qualifier
009	Invalid Value as Shown in the Reported Interchange Sender ID
010	Invalid Value as Shown in the Reported Interchange Receiver ID Qualifier
011	Invalid Value as Shown in the Reported Interchange Receiver ID
016	Trading Partnership not Established
017	Invalid Number of Included Groups Value
018	Invalid Control Structure
019	Improper (Premature) End-of-file (Transmission)
020	Duplicate Interchange Control Number
021	Invalid Data Element Separator
022	Invalid Component Element Separator
023	Failure to Transfer Interchange to the next Service Request Handler
031	Receiver Not On-line
032	Abnormal Conditions

Must Use TA304 I44 Reported Start Segment ID M AN 2/3

This contains the start segment ID of the original interchange, functional group or transaction set

For ANSI ASC X12 interchanges, the start segment ID is always ISA.

Must Use TA305 I45 Reported Control Number M AN 1/14

This is the control number value of the original interchange, functional group or transaction set

Cite the control number assigned in the original interchange control header (appearing in ISA13) for which notice is being provided. With this control number, the TA3 is linked to the original interchange envelope.

Must Use TA306 I46 Reported Date M AN 1/8

This is the date value of original interchange or functional group

Cite the date appearing in ISA09 of the interchange for which delivery notice is being provided.

Must Use TA307 I47 Reported Time M AN 1/8

This is the time value of original interchange or functional group

Cite the time appearing in ISA10 of the interchange for which delivery notice is being provided.

Must Use TA308 I48 Reported Interchange Sender ID Qualifier M AN 1/4

This is the sender ID qualifier value appearing in original interchange

Cite the value appearing in ISA05 of the interchange for which delivery notice is being provided.

Must Use TA309 I49 Reported Sender ID M AN 1/35

This is the sender ID value of original interchange or functional group

Cite the value appearing in ISA06 of the interchange for which delivery notice is being provided.

Must Use TA310 I50 Reported Interchange Receiver ID Qualifier M AN 1/4

This is the receiver ID qualifier value appearing in original interchange

Cite the value appearing in ISA07 of the interchange for which delivery notice is being provided.

Must Use TA311 I51 Reported Receiver ID M AN 1/35

This is the receiver ID value of original interchange or functional group

Cite the value appearing in ISA08 of the interchange for which delivery notice is being provided.

Must Use TA312 I40 Action Code M ID 2/2

This is a code indicating the action taken on the interchange or functional group by the service request handler or the receiver

AK	Transfer to the Next Service Request Handler has been Acknowledged
BH	Transfer to Service Request Handler not Capable of Reporting Further Status
DL	Delivered Interchange by Service Request Handler
PU	Purged by Interchange Receiver
RD	Redirected by Service Request Handler to an Alternate Receiver as Identified in the Reference Code
RF	Refused by Interchange Receiver
RJ	Rejected by Service Request Handler; See Error Reason Code for Cause
RT	Retrieved Interchange by Receiver
TR	Transferred to Next Service Request Handler by Service Request Handler, but not yet Acknowledged

Must Use TA313 I41 Action Date M DT 6/6

This is the UTC date when the service request handler took action on the reported interchange or functional group

Express the UTC (previously known as GMT) date in a six-position (YYMMDD) format.

Must Use TA314 I42 Action Time M TM 4/6

This is the UTC time when the service request handler took action on the reported interchange or functional group

Express the UTC (previously known as GMT) time in a four-position (HHMM) format.

Not Used TA315 I40 Action Code O ID 2/2

This is a code indicating the action taken on the interchange or functional group by the service request handler or the receiver

Refer to 003070 Data Element Dictionary for acceptable code values.

Not Used TA316 I41 Action Date O DT 6/6

This is the UTC date when the service request handler took action on the reported interchange or functional group

Not Used TA317 I42 Action Time O TM 4/6

This is the UTC time when the service request handler took action on the reported interchange or functional group

Not Used TA318 I52 First Reference ID Qualifier O AN 1/4

This is the ID qualifier appearing in original interchange

Not Used TA319 I53 First Reference ID O AN 1/14

This contains information from the original interchange, as defined by the First Reference ID Qualifier data element

Not Used TA320 I54 Second Reference ID Qualifier O AN 1/4

This contains ID qualifier information appearing in original interchange

Not Used TA321 I55 Second Reference ID O AN 1/14

This contains information from the original interchange, as defined by the Second Reference ID Qualifier data element

TA322 **I56** **Reference Code Qualifier** **X** **ID 2/2**

This is a code defining the information contained in the Reference Code data element

If TA312 is code RD, use TA322 and TA323 to identify the organization to which the interchange was redirected.

05 ID of Alternate Receiver to which Interchange Has Been Redirected

TA323 **I57** **Reference Code** **X** **AN 1/35**

This contains reference information exchanged between service request handlers concerning the reported interchange as defined by the corresponding Reference Code Qualifier data element

Cite the identifier of the organization to which the interchange was redirected. The orgainization shall be identified via a unique identifier from one of the sources listed as allowable codes in the ISA05 definition in section 10.6 of the Federal EDI Guidelines. The Data Universal Numbering System (D-U-N-S) number and D-U-N-S +4 are the prefered identifiers.

Not Used **TA324** **I56** **Reference Code Qualifier** **X** **ID 2/2**

This is a code defining the information contained in the Reference Code data element

Not Used **TA325** **I57** **Reference Code** **X** **AN 1/35**

This contains reference information exchanged between service request handlers concerning the reported interchange as defined by the corresponding Reference Code Qualifier data element

Not Used **TA326** **I56** **Reference Code Qualifier** **X** **ID 2/2**

This is a code defining the information contained in the Reference Code data element

Not Used **TA327** **I57** **Reference Code** **X** **AN 1/35**

This contains reference information exchanged between service request handlers concerning the reported interchange as defined by the corresponding Reference Code Qualifier data element

Segment: **GS** **Functional Group Header**

Usage: Optional

Max Use: 1

Purpose: To indicate the beginning of a functional group and to provide control information

Syntax Notes:

Semantic Notes: The data interchange control number GS06 in this header must be identical to the same data element in the associated functional group trailer, GE02.

Comments: A functional group of related transaction sets, within the scope of X12 standards, consists of a collection of similar transaction sets enclosed by a functional group header and a functional group trailer.

Notes: ***1. Use to identify the functional group containing one or more related transactions.***

2. Use to identify the specific implementation convention with which the transaction sets contained within the functional group envelope comply.

3. The version and release of the GS segment must be the same as the version and release of the transactions that follow it as specified in the Version / Release / Industry Identifier Code (GS08).

4. The GS segment represented here is valid for version 2003.

Data Element Summary

	Ref. Des.	Data Element	Name	Attributes
Must Use	**GS01**	**479**	**Functional Identifier Code** Code identifying a group of application related transaction sets ***Cite any valid code defined for data element 479 in the ASC X12 2003 Standards Data Element Dictionary providing a Federal implementation convention exists for the cited transaction set.***	**M ID 2/2**

Must Use	**GS02**	**142**	**Application Sender's Code**	**M**	**AN 2/12**

Code identifying party sending transmission .

1. Cite the sending application's identifier. This identifier must be unique within the domain of the sending application's translation point. Use of a Dun and Bradstreet number (DUNS) is recommended to provide universal uniqueness.

2. Transmit the required number of characters without leading or trailing blanks.

Must Use	**GS03**	**124**	**Application Receiver's Code**	**M**	**AN 2/12**

Code identifying party receiving transmission

1. Cite the receiving application's identifier. This identifier must be unique within the domain of the receiving application's translation point. Use of a Dun and Bradstreet number (DUNS) is recommended to provide universal uniqueness.

2. Transmit the required number of characters without leading or trailing blanks.

3. If the group contains PUBLIC transactions, enter the literal string 'PUBLIC'.

Must Use	**GS04**	**29**	**Data Interchange Date**	**M**	**DT 6/6**

Date sender generated a functional group of transaction sets.

1. Enter the UTC (previously known as GMT) date that this segment was created.

2. Express the date in a six-position (YYMMDD) format.

Must Use	**GS05**	**30**	**Data Interchange Time**	**M**	**TM 4/4**

Time (HHMM) when the sender generated a functional group of transaction sets (local time at sender's location).

1. Enter the UTC (previously known as GMT) time that this segment was created.

2. Express the time in a four-position (HHMM) format.

Must Use GS06 28 Data Interchange Control Number M N0 1/9

Assigned number originated and maintained by the sender

1. Originating activities may use any numbering scheme consistent with their business practices.

2. The scheme must provide sufficient uniqueness to identify each functional group. The Group Control Number value, together with the Application Sender's and Receiver's Codes, shall be unique within an extended time frame - such as a year.

Must Use GS07 455 Responsible Agency Code M ID 1/2

Code used in conjunction with Data Element 480 to identify the issuer of the standard

X Accredited Standards Committee X12

Must Use GS08 480 Version / Release / Industry Identifier Code M AN 1/12

Code indicating the version, release, subrelease, and industry identifier of the EDI standard being used. Positions 1-3, Major Version Number; Positions 4-6, Release Level of Version; Positions 7-12, Industry or Trade Association ID (optionally assigned by user).

Each Federal and DoD Implementation Convention, based on an ANSI ASC X12 transaction set, used by the government has a unique identifier specified as follow:

Positions 1 through 6: ANSI ASC X12 Version and Release number (e.g. 003010) upon which the IC is based.

Position 7: Organizational Scope

F = Federal

D = DOD

G = Government (transitional)

Positions 8 through 10: Transaction Set Identifier Code (e.g. 850).

Position 11: Variant: A character used to differentiate between different functional implementations of the same transaction set.

If the convention is not a variant, an underscore (_) will appear in this position.

Position 12: A sequential number starting with 0 and incremented by 1 each time the implementation convention is revised.

Segment: **GS** **Functional Group Header**

Usage: Optional

Max Use: 1

Purpose: To indicate the beginning of a functional group and to provide control information

Syntax Notes:

Semantic Notes: The data interchange control number GS06 in this header must be identical to the same data element in the associated functional group trailer, GE02.

Comments: A functional group of related transaction sets, within the scope of X12 standards, consists of a collection of similar transaction sets enclosed by a functional group header and a functional group trailer.

Notes: ***1. Use to identify the functional group containing one or more related transactions.***

2. Use to identify the specific implementation convention with which the transaction sets contained within the functional group envelope comply.

3. The version and release of the GS segment must be the same as the version and release of the transactions that follow it as specified in the Version / Release / Industry Identifier Code (GS08).

4. The GS segment represented here is valid for version 3010.

Data Element Summary

	Ref. Des.	Data Element	Name	Attributes
Must Use	**GS01**	**479**	**Functional Identifier Code** Code identifying a group of application related transaction sets ***Cite any valid code defined for data element 479 in the ASC X12 3010 Standards Data Element Dictionary providing a Federal implementation convention exists for the cited transaction set.***	**M ID 2/2**

Must Use	**GS02**	**142**	**Application Sender's Code**	**M**	**AN 2/12**

Code identifying party sending transmission .

1. Cite the sending application's identifier. This identifier must be unique within the domain of the sending application's translation point. Use of a Dun and Bradstreet number (DUNS) is recommended to provide universal uniqueness.

2. Transmit the required number of characters without leading or trailing blanks.

Must Use	**GS03**	**124**	**Application Receiver's Code**	**M**	**AN 2/12**

Code identifying party receiving transmission

1. Cite the receiving application's identifier. This identifier must be unique within the domain of the receiving application's translation point. Use of a Dun and Bradstreet number (DUNS) is recommended to provide universal uniqueness.

2. Transmit the required number of characters without leading or trailing blanks.

3. If the group contains PUBLIC transactions, enter the literal string 'PUBLIC'.

Must Use	**GS04**	**29**	**Group Date**	**M**	**DT 6/6**

Date sender generated a functional group of transaction sets.

1. Enter the UTC (previously known as GMT) date that this segment was created.

2. Express the date in a six-position (YYMMDD) format.

Must Use	**GS05**	**30**	**Group Time**	**M**	**TM 4/4**

Time (HHMM) when the sender generated a functional group of transaction sets (local time at sender's location).

1. Enter the UTC (previously known as GMT) time that this segment was created.

2. Express the time in a four-position (HHMM) format.

Must Use GS06 28 Group Control Number M N0 1/9

Assigned number originated and maintained by the sender

1. Originating activities may use any numbering scheme consistent with their business practices.

2. The scheme must provide sufficient uniqueness to identify each functional group. The Group Control Number value, together with the Application Sender's and Receiver's Codes, shall be unique within an extended time frame - such as a year.

Must Use GS07 455 Responsible Agency Code M ID 1/2

Code used in conjunction with Data Element 480 to identify the issuer of the standard

X Accredited Standards Committee X12

Must Use GS08 480 Version / Release / Industry Identifier Code M AN 1/12

Code indicating the version, release, subrelease, and industry identifier of the EDI standard being used. Positions 1-3, Major Version Number; Positions 4-6, Release Level of Version; Positions 7-12, Industry or Trade Association ID (optionally assigned by user).

Each Federal and DoD Implementation Convention, based on an ANSI ASC X12 transaction set, used by the government has a unique identifier specified as follow:

Positions 1 through 6: ANSI ASC X12 Version and Release number (e.g. 003010) upon which the IC is based.

Position 7: Organizational Scope

F = Federal

D = DOD

G = Government (transitional)

Positions 8 through 10: Transaction Set Identifier Code (e.g. 850).

Position 11: Variant: A character used to differentiate between different functional implementations of the same transaction set.

If the convention is not a variant, an underscore (_) will appear in this position.

Position 12: A sequential number starting with 0 and incremented by 1 each time the implementation convention is revised.

Segment: **GS** **Functional Group Header**

Usage: Optional

Max Use: 1

Purpose: To indicate the beginning of a functional group and to provide control information

Syntax Notes:

Semantic Notes:

1 GS04 is the group date.

2 GS05 is the group time.

3 The data interchange control number GS06 in this header must be identical to the same data element in the associated functional group trailer, GE02.

Comments:

1 A functional group of related transaction sets, within the scope of X12 standards, consists of a collection of similar transaction sets enclosed by a functional group header and a functional group trailer.

Notes:

1. Use to identify the functional group containing one or more related transactions.

2. Use to identify the specific implementation convention with which the transaction sets contained within the functional group envelope comply.

3. The version and release of the GS segment must be the same as the version and release of the transactions that follow it as specified in the Version / Release / Industry Identifier Code (GS08).

4. The GS segment represented here is valid for version 3040 through 3070.

Data Element Summary

	Ref. Des.	Data Element	Name	Attributes
Must Use	**GS01**	**479**	**Functional Identifier Code** Code identifying a group of application related transaction sets ***Cite any valid code defined for data element 479 in the ASC X12 3040 through 3070 (as applicable) Standards Data Element Dictionary providing a Federal implementation convention exists for the cited transaction set.***	**M ID 2/2**
Must Use	**GS02**	**142**	**Application Sender's Code** Code identifying party sending transmission; codes agreed to by trading partners ***1. Cite the sending application's identifier. This identifier must be unique within the domain of the sending application's translation point. Use of a Dun and Bradstreet number (DUNS or DUNS+4) is recommended to provide universal uniqueness.*** ***2. Transmit the required number of characters without leading or trailing blanks.***	**M AN 2/15**
Must Use	**GS03**	**124**	**Application Receiver's Code** Code identifying party receiving transmission. Codes agreed to by trading partners ***1. Cite the receiving application's identifier. This identifier must be unique within the domain of the receiving application's translation point. Use of a Dun and Bradstreet number (D-U-N-S or D-U-N-S+4) is recommended to provide universal uniqueness.*** ***2. Transmit the required number of characters without leading or trailing blanks.*** ***3. If the group contains PUBLIC transactions, enter the literal string 'PUBLIC'.***	**M AN 2/15**

Must Use	**GS04**	**373**	**Date**	**M**	**DT 6/6**

Date (YYMMDD)

1. Enter the UTC (previously known as GMT) date that this segment was created.

2. Express the date in a six-position (YYMMDD) format.

Must Use	**GS05**	**337**	**Time**	**M**	**TM 4/8**

Time expressed in 24-hour clock time as follows: HHMM, or HHMMSS, or HHMMSSD, or HHMMSSDD, where H = hours (00-23), M = minutes (00-59), S = integer seconds (00-59) and DD = decimal seconds; decimal seconds are expressed as follows: D = tenths (0-9) and DD = hundredths (00-99)

1. Enter the UTC (previously known as GMT) time that this segment was created.

2. Express the time in a four-position (HHMM) format.

Must Use	**GS06**	**28**	**Group Control Number**	**M**	**N0 1/9**

Assigned number originated and maintained by the sender

1. Originating activities may use any numbering scheme consistent with their business practices.

2. The scheme must provide sufficient uniqueness to identify each functional group. The Group Control Number value, together with the Application Sender's and Receiver's Codes, shall be unique within an extended time frame - such as a year.

Must Use	**GS07**	**455**	**Responsible Agency Code**	**M**	**ID 1/2**

Code used in conjunction with Data Element 480 to identify the issuer of the standard

X Accredited Standards Committee X12

Must Use	**GS08**	**480**	**Version / Release / Industry Identifier Code**	**M**	**AN 1/12**

Code indicating the version, release, subrelease, and industry identifier of the EDI standard being used, including the GS and

GE segments; if code in DE455 in GS segment is X, then in DE 480 positions 1-3 are the version number; positions 4-6 are the release and subrelease, level of the version; and positions 7-12 are the industry or trade association identifiers (optionally assigned by user); if code in DE455 in GS segment is T, then other formats are allowed

Each Federal and DoD Implementation Convention, based on an ANSI ASC X12 transaction set, used by the government has a unique identifier specified as follow:

Positions 1 through 6: ANSI ASC X12 Version and Release number (e.g. 003010) upon which the IC is based.

Position 7: Organizational Scope

F = Federal

D = DOD

G = Government (transitional)

Positions 8 through 10: Transaction Set Identifier Code (e.g. 850).

Position 11: Variant: A character used to differentiate between different functional implementations of the same transaction set.

If the convention is not a variant, an underscore (_) will appear in this position.

Position 12: A sequential number starting with 0 and incremented by 1 each time the implementation convention is revised.

Segment: **S1S** **Security Header Level 1**

Usage: Optional

Max Use: 1

Purpose: To initiate the beginning of a secured area and to provide the parameters needed for authentication or encryption of a functional group

Syntax Notes:

1 If either S1S04 or S1S05 is present, then the other is required.

2 If any of S1S06 S1S07 S1S08 or S1S09 is present, then all are required.

Semantic Notes:

1 If S1S01 is ``AA" or ``BB", S1S04 is required.

If S1S01 is ``BB" or ``EE", S1S06 is required.

Comments:

Notes:

1. X9 has a minimum length of 4 characters for S1S02 (the security originator); no mechanism, or registration method is provided by X9 or X12 to guarantee the uniqueness of the identifier

2. X9 has a minimum length of 4 characters for S1S03 (the security recipient); no mechanism, or registration method is provided by X9 or X12 to guarantee the uniqueness of the identifier

3. The S1S segment represented here is only valid for versions 3040 and 3050.

Data Element Summary

	Ref. Des.	Data Element	Name	Attributes
Must Use	**S1S01**	**990**	**Security Type** Code identifying the security algorithms and methods employed for this level of interchange. EE Encryption, No Authentication	**M ID 2/2**

Must Use **S1S02** **824** **Security Originator Name** **M** **AN 4/16**

Unique designation (identity) of the cryptographic process that performs authentication or encryption on data to be interchanged, or originates a cryptographic service message

Note: X9 has a minimum length of 4 characters for the security originator; no mechanism, or registration method is provided by X9 or X12 to guarantee the uniqueness of the identifier

Must Use **S1S03** **825** **Security Recipient Name** **M** **AN 4/16**

Unique designation (identity) of the cryptographic process that performs authentication or decryption on received data, or is the destination of a cryptographic service message

Note: X9 has a minimum length of 4 characters for the security recipient; no mechanism, or registration method is provided by X9 or X12 to guarantee the uniqueness of the identifier

S1S04 **991** **Authentication Key Name** **X** **AN 1/16**

Name of the key used for authentication. This name is mutually known to the security originator and the security recipient, is unique for this relationship, and allows a particular key to be specified.

S1S05 **992** **Authentication Service Code** **X** **ID 1/1**

Authentication option

1	ANSI X9.9 Binary Data
2	ANSI X9.9 Coded Character Set, Entire Message, No Editing Standard value for ANSI X9.17 authentication, with the data element separator expressed as an asterisk and the segment terminator expressed as a linefeed character for the calculation of the message authentication code (MAC)

S1S06 **993** **Encryption Key Name** **X** **AN 1/16**

Name of the key used for encryption. This name is mutually known to the security originator and the security recipient, is

unique for this relationship, and allows a particular key to be specified.

S1S07 994 Encryption Service Code X ID 1/3

Coded values representing options for encryption processing. The code defines the encryption mode and the transmission filter specification for filtering binary ciphertext data into transmittable text.

21	ANSI X9.23 Cipher Block Chaining (CBC), Hexadecimal Filter
22	ANSI X9.23 Cipher Block Chaining (CBC), ASCII Filter
41	ANSI X9.23 CFB-8 (Cipher Feedback), Hexadecimal Filter
42	ANSI X9.23 CFB-8 (Cipher Feedback), ASCII Filter

S1S08 995 Length of Data (LOD) X N 1/18

Length of data is the number of character positions of the encrypted, filtered text.

S1S09 996 Initialization Vector (IV) X AN 16/16

The archival representation of a 64-bit value expressed in hexadecimal notation as 16 ASCII characters from the set of characters (0..9, A..F); the 64-bit value is used as a starting point for encryption of a data sequence to increase security by introducing cryptographic variance and to synchronize cryptographic equipment; a new Initialization Vector (IV) shall be used for each message; the IV shall not be intentionally reused; the 64-bit binary value, not its ASCII representation, is used for the cryptographic process; in the interchange process, the resultant encrypted and filtered 64-bit IV is sent; the hexadecimal notation is the representation for archiving purposes; the IV shall be a random or pseudo-random number; when encrypted, the IV must be decrypted using the Electronic Code Book (ECB) mode and the same key used to encrypt the message

Segment: **S1S** **Security Header Level 1**

Usage: Optional

Max Use: 1

Purpose: To initiate the beginning of a secured area and to provide the parameters needed for authentication or encryption of a functional group

Syntax Notes:

1 If either S1S04 or S1S05 is present, then the other is required.

2 If any of S1S06 S1S07 S1S08 or S1S09 is present, then all are required.

3 If either C03204 or C03205 is present, then the other is required.

4 If either C03206 or C03207 is present, then the other is required.

Semantic Notes:

1 If S1S01 is "AA", "BB", "AC" or "BC", then S1S04 is required.

If S1S01 is "BB", "EE", "AC" or "EC", then S1S06 is required.

Comments:

1 X9 has a required minimum length of four characters for S1S02 (security originator). No mechanism, or registration method, is provided by X9 or X12 to guarantee uniqueness of the identifier.

2 X9 has a required minimum length of four characters for S1S03 (security recipient). No mechanism, or registration method, is provided by X9 or X12 to guarantee uniqueness of the identifier.

3 In S1S04, the special name "01234567890ABCDEF" is reserved for the hexadecimal value 01234567890ABCDEF (i.e., a fixed, nonsecret value) to provide a well-known value for data-integrity testing only.

Notes:

1. X9 has a minimum length of 4 characters for S1S02 (the security originator); no mechanism, or registration method is provided by X9 or X12 to guarantee the uniqueness of the identifier

2. X9 has a minimum length of 4 characters for S1S03 (the security recipient); no mechanism, or registration method is provided by X9 or X12 to guarantee the uniqueness of the identifier

3. The S1S segment represented here is only valid for versions 3060 and 3070.

Data Element Summary

	Ref. Des.	Data Element	Name	Attributes
Must Use	**S1S01**	**990**	**Security Type** Code identifying the security algorithms and methods applied for this level of interchange EC — No Authentication, Compression, Encryption EE — No Authentication, No Compression, Encryption	**M ID 2/2**
Must Use	**S1S02**	**824**	**Security Originator Name** Unique designation (identity) of the cryptographic process that performs authentication or encryption on data to be interchanged, or originates a cryptographic service message Note: X9 has a minimum length of 4 characters for the security originator; no mechanism, or registration method is provided by X9 or X12 to guarantee the uniqueness of the identifier	**M AN 1/64**
	S1S03	**825**	**Security Recipient Name** Unique designation (identity) of the cryptographic process that performs authentication or decryption on received data, or is the destination of a cryptographic service message Note: X9 has a minimum length of 4 characters for the security recipient; no mechanism, or registration method is provided by X9 or X12 to guarantee the uniqueness of the identifier	**O AN 1/64**
	S1S04	**991**	**Authentication Key Name** Name of the key used for authentication; this name is mutually known to the security originator and the security recipient, is unique for this relationship, and is intended to allow the changing of the key from time to time Note: The special key name "0123456789ABCDEF" is reserved for the hexidecimal value 0123456789ABCDEF (i.e. a fixed non-secret value) to provide a well-known value for data integrity testing only)	**X AN 1/64**

	S1S05	**992**	**Authentication Service Code**	**X**	**ID 1/1**
			Authentication options 4 MD5 Hash 5 SHA Hash		
	S1S06	**C031**	**Encryption Key Information**	**X**	
			Information needed to identify or obtain the encryption key		
Must Use	**C03101**	**993**	**Encryption Key Name**	**M**	**AN 1/64**
			Name of the key used for encryption; this name is mutually known to the security originator and the security recipient, is unique for this relationship, and is intended to allow the changing of the key from time to time Note: If any of the optional fields are present, the Key Name should contain either "PUBLIC" if a public key is being used to encrpyt the one-time key or the actual name of the asymmetric key-encrypting-key used to encrypt the one-time key.		
	C03102	**1564**	**Protocol ID**	**O**	**ID 3/3**
			Code specifying protocol used to encrypt the session key KEA Key Encryption Algorithm RSA RSA Algorithm		
	C03103	**1565**	**Look-up Value**	**O**	**AN 1/512**
			Value used to identify a certificate containing the public key used to encrypt the one-time key		
	C03104	**1566**	**Keying Material**	**O**	**AN 1/512**
			Additional material required for decrypting the one-time key		
	C03105	**1567**	**One-time Encryption Key**	**O**	**AN 1/512**
			Hexadecimally filtered encrypted one-time key		

	S1S07	**C032**	**Encryption Service Information**	**X**	

Information required by the encryption operation

Must Use	**C03201**	**994**	**Encryption Service Code**	**M**	**ID 1/3**

Coded values representing options for encryption processing, including the use of compression and filtering; the code either defines the encryption mode and the transmission filter specification for filtering binary data into transmittable text or specifics that the following subelements define these values

21	ANSI X9.23 Cipher Block Chaining (CBC), Hexadecimal Filter
22	ANSI X9.23 Cipher Block Chaining (CBC), ASCII Filter
41	ANSI X9.23 CFB-8 (Cipher Feedback), Hexadecimal Filter
42	ANSI X9.23 CFB-8 (Cipher Feedback), ASCII Filter

	C03202	**1568**	**Algorithm ID**	**O**	**ID 3/3**

Algorithm used for Encryption

DE3	Triple DEA
DES	Data Encryption Standard (Same as DEA)
	As specified in FIPS 46-2.
SKJ	Skipjack

	C03203	**1569**	**Algorithm Mode of Operation**	**O**	**ID 3/3**

Mode of Operation of the Encryption Algorithm

CBC	Cipher Block Chaining

	C03204	**1570**	**Filter ID Code**	**X**	**ID 3/3**

Code specifying the type of filter used to convert data code values

ASB	ASCII-Baudot Filter
ASC	ASCII Filter
HDC	Hexadecimal Filter
UUE	Uuencoding
ZZZ	Mutually Defined

Use to indicate Base 64.

C03205 799 Version Identifier X AN 1/30

Revision level of a particular format, program, technique or algorithm

C03206 1571 Compression ID X ID 3/3

Type of Compression Used

913	X9E13 Compression as defined by X9.32
ZZZ	Mutually Defined

Use to indicate that each block has been compressed by using a combination of the Lempel-Ziv LZ77 algorithm and Huffman coding, in accordance with the Internet Engineering Task Force (IETF) Request for Comments (RFC) 1951 format.

C03207 799 Version Identifier X AN 1/30

Revision level of a particular format, program, technique or algorithm

Cite the version of the compression algorithm cited in S1S07 (C03206) above.

S1S08 995 Length of Data X N 1/18

Length of data is the number of character positions of the compressed or encrypted/filtered text; when data is plain text, this field shall be absent

S1S09	**996**	**Initialization Vector**	**X**	**AN 16/16**

The archival representation of a 64-bit value expressed in hexadecimal notation as 16 ASCII characters from the set of characters (0..9, A..F); the 64-bit value is used as a starting point for encryption of a data sequence to increase security by introducing cryptographic variance and to synchronize cryptographic equipment; a new Initialization Vector (IV) shall be used for each message; the IV shall not be intentionally reused; the 64-bit binary value, not its ASCII representation, is used for the cryptographic process; in the interchange process, the resultant encrypted and filtered 64-bit IV is sent; the hexadecimal notation is the representation for archiving purposes; the IV shall be a random or pseudo-random number; when encrypted, the IV must be decrypted using the Electronic Code Book (ECB) mode and the same key used to encrypt the message

Segment: **S2S** **Security Header Level 2**

Usage: Optional

Max Use: 1

Purpose: To initiate the beginning of a secured area and to provide the parameters needed for authentication or encryption of a transaction set

Syntax Notes: **1** If either S2S04 or S2S05 is present, then the other is required.

2 If any of S2S06 S2S07 S2S08 or S2S09 is present, then all are required.

Semantic Notes: **1** If S2S01 is ``AA" or ``BB", S2S04 is required.

If S2S01 is ``BB" or ``EE", S2S06 is required.

Comments:

Notes: ***1. X9 has a minimum length of 4 characters for S2S02 (the security originator); no mechanism, or registration method is provided by X9 or X12 to guarantee the uniqueness of the identifier***

2. X9 has a minimum length of 4 characters for S2S03 (the security recipient); no mechanism, or registration method is provided by X9 or X12 to guarantee the uniqueness of the identifier.

3. The S2S segment represented here is only valid for versions 3040 and 3050.

Data Element Summary

	Ref. Des.	Data Element	Name	Attributes
Must Use	**S2S01**	**990**	**Security Type** Code identifying the security algorithms and methods employed for this level of interchange. EE Encryption, No Authentication	**M ID 2/2**

Must Use	**S2S02**	**824**	**Security Originator Name**	**M**	**AN 4/16**

Unique designation (identity) of the cryptographic process that performs authentication or encryption on data to be interchanged, or originates a cryptographic service message

Note: X9 has a minimum length of 4 characters for the security originator; no mechanism, or registration method is provided by X9 or X12 to guarantee the uniqueness of the identifier

Must Use	**S2S03**	**825**	**Security Recipient Name**	**M**	**AN 4/16**

Unique designation (identity) of the cryptographic process that performs authentication or decryption on received data, or is the destination of a cryptographic service message

Note: X9 has a minimum length of 4 characters for the security recipient; no mechanism, or registration method is provided by X9 or X12 to guarantee the uniqueness of the identifier

	S2S04	**991**	**Authentication Key Name**	**X**	**AN 1/16**

Name of the key used for authentication. This name is mutually known to the security originator and the security recipient, is unique for this relationship, and allows a particular key to be specified.

	S2S05	**992**	**Authentication Service Code**	**X**	**ID 1/1**

Authentication option

	S2S06	**993**	**Encryption Key Name**	**X**	**AN 1/16**

Name of the key used for encryption. This name is mutually known to the security originator and the security recipient, is unique for this relationship, and allows a particular key to be specified.

	S2S07	**994**	**Encryption Service Code**	**X**	**ID 1/3**

Coded values representing options for encryption processing. The code defines the encryption mode and the transmission filter specification for filtering binary ciphertext data into transmittable text.

21	ANSI X9.23 Cipher Block Chaining (CBC), Hexadecimal Filter

	22	ANSI X9.23 Cipher Block Chaining (CBC), ASCII Filter
	41	ANSI X9.23 CFB-8 (Cipher Feedback), Hexadecimal Filter
	42	ANSI X9.23 CFB-8 (Cipher Feedback), ASCII Filter

S2S08 995 Length of Data (LOD) X N 1/18

Length of data is the number of character positions of the encrypted, filtered text.

S2S09 996 Initialization Vector (IV) X AN 16/16

The archival representation of a 64-bit value expressed in hexadecimal notation as 16 ASCII characters from the set of characters (0..9, A..F); the 64-bit value is used as a starting point for encryption of a data sequence to increase security by introducing cryptographic variance and to synchronize cryptographic equipment; a new Initialization Vector (IV) shall be used for each message; the IV shall not be intentionally reused; the 64-bit binary value, not its ASCII representation, is used for the cryptographic process; in the interchange process, the resultant encrypted and filtered 64-bit IV is sent; the hexadecimal notation is the representation for archiving purposes; the IV shall be a random or pseudo-random number; when encrypted, the IV must be decrypted using the Electronic Code Book (ECB) mode and the same key used to encrypt the message

Segment: **S2S** **Security Header Level 2**

Usage: Optional

Max Use: 1

Purpose: To initiate the beginning of a secured area and to provide the parameters needed for authentication or encryption of a transaction set

Syntax Notes:

1 If either S2S04 or S2S05 is present, then the other is required.

2 If any of S2S06 S2S07 S2S08 or S2S09 is present, then all are required.

3 If either C03204 or C03205 is present, then the other is required.

4 If either C03206 or C03207 is present, then the other is required.

Semantic Notes:

1 If S2S01 is "AA", "BB", "AC" or "BC", then S2S04 is required.

If S2S01 is "BB", "EE", "AC" or "EC", then S2S06 is required.

Comments:

1 X9 has a required minimum length of four characters for S2S02 (security originator). No mechanism, or registration method, is provided by X9 or X12 to guarantee uniqueness of the identifier.

2 X9 has a required minimum length of four characters for S2S03 (security recipient). No mechanism, or registration method, is provided by X9 or X12 to guarantee uniqueness of the identifier.

3 In S2S04 the special name "01234567890ABCDEF" is reserved for the hexadecimal value 01234567890ABCDEF (i.e., a fixed nonsecret value) to provide a well-known value for data-integrity testing only.

Notes:

1. X9 has a minimum length of 4 characters for S2S02 (the security originator); no mechanism, or registration method is provided by X9 or X12 to guarantee the uniqueness of the identifier

2. X9 has a minimum length of 4 characters for S2S03 (the security recipient); no mechanism, or registration method is provided by X9 or X12 to guarantee the uniqueness of the identifier.

3. The S2S segment represented here is only valid for versions 3060 and 3070.

Data Element Summary

	Ref. Des.	Data Element	Name	Attributes
Must Use	**S2S01**	**990**	**Security Type** Code identifying the security algorithms and methods applied for this level of interchange EC No Authentication, Compression, Encryption EE No Authentication, No Compression, Encryption	**M ID 2/2**
Must Use	**S2S02**	**824**	**Security Originator Name** Unique designation (identity) of the cryptographic process that performs authentication or encryption on data to be interchanged, or originates a cryptographic service message Note: X9 has a minimum length of 4 characters for the security originator; no mechanism, or registration method is provided by X9 or X12 to guarantee the uniqueness of the identifier	**M AN 1/64**
	S2S03	**825**	**Security Recipient Name** Unique designation (identity) of the cryptographic process that performs authentication or decryption on received data, or is the destination of a cryptographic service message Note: X9 has a minimum length of 4 characters for the security recipient; no mechanism, or registration method is provided by X9 or X12 to guarantee the uniqueness of the identifier	**O AN 1/64**
	S2S04	**991**	**Authentication Key Name** Name of the key used for authentication; this name is mutually known to the security originator and the security recipient, is unique for this relationship, and is intended to allow the changing of the key from time to time Note: The special key name "0123456789ABCDEF" is reserved for the hexidecimal value 0123456789ABCDEF (i.e. a fixed non-secret value) to provide a well-known value for data integrity testing only)	**X AN 1/64**

	S2S05	**992**	**Authentication Service Code**	**X**	**ID 1/1**
			Authentication options		
			4 MD5 Hash		
			5 SHA Hash		
	S2S06	**C031**	**Encryption Key Information**	**X**	
			Information needed to identify or obtain the encryption key		
Must Use	**C03101**	**993**	**Encryption Key Name**	**M**	**AN 1/64**
			Name of the key used for encryption; this name is mutually known to the security originator and the security recipient, is unique for this relationship, and is intended to allow the changing of the key from time to time		
			Note: If any of the optional fields are present, the Key Name should contain either "PUBLIC" if a public key is being used to encrypt the one-time key or the actual name of the asymmetric key-encrypting-key used to encrypt the one-time key.		
	C03102	**1564**	**Protocol ID**	**O**	**ID 3/3**
			Code specifying protocol used to encrypt the session key		
			KEA Key Encryption Algorithm		
			RSA RSA Algorithm		
	C03103	**1565**	**Look-up Value**	**O**	**AN 1/512**
			Value used to identify a certificate containing the public key used to encrypt the one-time key		
	C03104	**1566**	**Keying Material**	**O**	**AN 1/512**
			Additional material required for decrypting the one-time key		
	C03105	**1567**	**One-time Encryption Key**	**O**	**AN 1/512**
			Hexadecimally filtered encrypted one-time key		

	S2S07	**C032**	**Encryption Service Information**	**X**	
			Information required by the encryption operation		
Must Use	**C03201**	**994**	**Encryption Service Code**	**M**	**ID 1/3**
			Coded values representing options for encryption processing, including the use of compression and filtering; the code either defines the encryption mode and the transmission filter specification for filtering binary data into transmittable text or specifies that the following subelements define these values		
			21 ANSI X9.23 Cipher Block Chaining (CBC), Hexadecimal Filter		
			22 ANSI X9.23 Cipher Block Chaining (CBC), ASCII Filter		
			41 ANSI X9.23 CFB-8 (Cipher Feedback), Hexadecimal Filter		
			42 ANSI X9.23 CFB-8 (Cipher Feedback), ASCII Filter		
	C03202	**1568**	**Algorithm ID**	**O**	**ID 3/3**
			Algorithm used for Encryption		
			DE3 Triple DEA		
			DES Data Encryption Standard (Same as DEA)		
			As specified in FIPS 46-2.		
			SKJ Skipjack		
	C03203	**1569**	**Algorithm Mode of Operation**	**O**	**ID 3/3**
			Mode of Operation of the Encryption Algorithm		
			CBC Cipher Block Chaining		
	C03204	**1570**	**Filter ID Code**	**X**	**ID 3/3**
			Code specifying the type of filter used to convert data code values		

ASB	ASCII-Baudot Filter	
ASC	ASCII Filter	
HDC	Hexadecimal Filter	
UUE	Uuencoding	
ZZZ	Mutually Defined	

Use to indicate Base 64.

C03205 799 Version Identifier X AN 1/30

Revision level of a particular format, program, technique or algorithm

C03206 1571 Compression ID X ID 3/3

Type of Compression Used

913	X9E13 Compression as defined by X9.32
ZZZ	Mutually Defined

Use to indicate that each block has been compressed by using a combination of the Lempel-Ziv LZ77 algorithm and Huffman coding, in accordance with the Internet Engineering Task Force (IETF) Request for Comments (RFC) 1951 format.

C03207 799 Cite the version of the compression algorithm cited in S1S07 (C03206) above. X AN 1/30

Revision level of a particular format, program, technique or algorithm

Cite the version of the compression algorithm cited in S2S07 (C03206) above.

S2S08 995 Length of Data X N 1/18

Length of data is the number of character positions of the compressed or encrypted/filtered text; when data is plain text, this field shall be absent

S2S09 **996** **Initialization Vector** **X** **AN 16/16**

The archival representation of a 64-bit value expressed in hexadecimal notation as 16 ASCII characters from the set of characters (0..9, A..F); the 64-bit value is used as a starting point for encryption of a data sequence to increase security by introducing cryptographic variance and to synchronize cryptographic equipment; a new Initialization Vector (IV) shall be used for each message; the IV shall not be intentionally reused; the 64-bit binary value, not its ASCII representation, is used for the cryptographic process; in the interchange process, the resultant encrypted and filtered 64-bit IV is sent; the hexadecimal notation is the representation for archiving purposes; the IV shall be a random or pseudo-random number; when encrypted, the IV must be decrypted using the Electronic Code Book (ECB) mode and the same key used to encrypt the message

Segment: **S2A** **Assurance Level 2**

Usage: Optional

Max Use: 1

Purpose: To allow for multiple assurances at the ST/SE level

Syntax Notes:

1 If C02804 is present, then C02803 is required.

2 If C02806 is present, then C02805 is required.

3 If C02808 is present, then C02807 is required.

4 If C02810 is present, then C02809 is required.

5 If C02812 is present, then C02811 is required.

6 If C02814 is present, then C02813 is required.

7 If C02816 is present, then C02815 is required.

8 If C02818 is present, then C02817 is required.

9 If C02820 is present, then C02819 is required.

Semantic Notes:

Comments:

1 X9 has a required minimum length of four characters for S2A04 (security originator). No mechanism, or registration method, is provided by X9 or X12 to guarantee uniqueness of the identifier.

2 X9 has a required minimum length of four characters for S2A05 (security recipient). No mechanism, or registration method, is provided by X9 or X12 to guarantee uniqueness of the identifier.

3 The date/time stamp may determine which of several key values apply, depending on start and expiration dates of different key values that may share the same keyname.

4 Key distribution is performed by other means and thus only onetime keys are allowed in S2A09.

The use of particular codes and corresponding values in S2A09 is dependent on the exigencies of the various crytographic algorithms.

Notes: ***1. Assurance (Digital Signature) segments (S2A/SVA) are not part of the control envelope structure. When used, insert the S2A/SVA segment pair(s) immediately preceding the SE segment of the transaction set for which assurance is being provided. See Section 10.5.3 of the Federal Implementation Guidelines.***

2. The S2A segment represented here is only valid for versions 3060 and 3070.

Data Element Summary

Ref. Des.	Data Element	Name	Attributes
Must Use	**S2A01**	**1432** **Business Purpose of Assurance**	**M ID 3/3**
		The stated business purpose for appending the assurance to an existing secured-entity (whether functional group or transaction set); the codes represent the intention of the business or application that has control over the assurance originator	
		ASG Authorization Signature Appropriate to this Document	
		CSG Authorization Co-signature Appropriate to this Document	
Must Use	**S2A02**	**C034** **Computation Methods**	**M**
		Algorithms used to calculate an assurance	
Must Use	**C03401**	**1574** **Assurance Algorithm**	**M ID 3/3**
		Code specifying the algorithm used to compute the assurance token	
		DSS Digital Signature Standard	
		As specified in FIPS 186.	
		RSA RSA	
Must Use	**C03402**	**1575** **Hashing Algorithm**	**M ID 3/3**
		Code specifying the algorithm used to compute the assurance digest	

			MD5	MD5		
			SHA	Secure hash algorithm		
Must Use	**S2A03**	**1434**	**Domain of Computation of Assurance Digest**		**M**	**ID 1/2**

The bounds of the text, whether contiguous or not, over which the computation of the Assurance Token is computed using the defined methodology of computation and any relevant Assurance Token parameters; the "body" is either a transaction set (beginning with the ST and including all segments up to the first S2A segment, but excluding any S2S segment) or functional group (beginning with the GS and including all transaction sets up to the first S1A segment, but excluding any S1S segment

"This Assurance" is defined as from the "S" in S1A or S2A up to and including the data element separator preceeding the assurance digest

"Previous Assurance(s)" is defined as including the entire S1A or S2A segment and the entire SVA that follows the included S1A or S2A

Refer to 003060 Data Element Dictionary for acceptable code values.

	S2A04	**1435**	**Assurance Originator**	**O**	**AN 1/64**

Unique designation (identity) of the cryptographic process that performs the stated assurance on data to be interchanged

Note: X9 has a required minimum length of 4 characters for a security originator; no mechanism, or registration method, is provided by X9 or X12 to guarantee uniqueness of the identifier

	S2A05	**1436**	**Assurance Recipient**	**O**	**AN 1/64**

Unique designation (identity) of the cryptographic process that performs validation of the stated assurance on received data. In the absence of an Assurance Recipient all potenial receivers will often be able to validate the assurance because the cryptographic technique is based on a "public" (as opposed to "secret") technology

Note: X9 has required minimum length of 4 characters for a security recipient; no mechanism, or registration method, is pro-

vided by X9 or X12 to guarantee uniqueness of the identifier

	S2A06	**1443**	**Assurance Reference Number**	**O**	**AN 1/35**

Alphanumeric reference number issued by security assurance originator for the particular assurance in which it occurs; unique when used in combination with security originator data element

	S2A07	**1437**	**Date/Time Reference**	**O**	**AN 17/25**

Date/time stamp in format as follows:

YYYYMMDDHHNNSSTTTZZZ+XXXX, where YYYY = 4 digit year (with leading century), MM = month of year (01..12), DD = day of month (01..31), HH = hour of day in 24-hour format (00..23), NN = minutes of the hour (00-59), SS = second of hour (00..59), TTT = [optional] milli-seconds (000..999), ZZZ = [optional] three character, nominal time zone indicator (including daylight savings time indicator) and XXXXX = 3-5 digit (including leading + or - sign) offset of time to universal time, with three position format indicating hours-offset for whole hours, and five position format indicating hours and minutes offset where this is necessary. For example:

199306152213300CDT+0930 which represents 15 June 1993, 22:13 (10:13pm), Central Daylight Time (Nominal Value "CDT"), in a time zone that is offset + 9:30 from Universal Time (Australia)

	S2A08	**1438**	**Assurance Text**	**O**	**AN 1/64**

Any text needed to convey the name of a signatory, registration number, certification number, or other assurance-originator defined or mutually-agreed business text related to the specific assurance; this text is not defined for X12 purposes and thus functions technically as "free form text" though it may have structure that is defined by the assurance originator, an industry group, a governmental agency, or bi-laterally between assurance originator and assurance recipient

	S2A09	**C028**	**Assurance Token Parameters**	**O**	

Parameters needed to calculate the Assurance Token

Must Use	**C02801**	**1439**	**Assurance Token Parameter Code**	**M**	**ID 2/2**

A code specifying the type of Assurance Token Parameter

CI	Certification Authority ID
EK	Key Value - One-Time Key
KN	Key Name
NT	Notarization
OD	Key-Encrypting-Key for One-Time Key
UI	User ID

Must Use C02802 1442 Assurance Token Parameter Value M AN 1/64

A value of a parameter, usually specifying one or more options, required for the proper operation of the cryptographic algorithm used to compute the Assurance Token; depending on the algorithm used, one or more values may be required

Not Used C02803 1439 Assurance Token Parameter Code X ID 2/2

A code specifying the type of Assurance Token Parameter

Not Used C02804 1442 Assurance Token Parameter Value O AN 1/64

A value of a parameter, usually specifying one or more options, required for the proper operation of the cryptographic algorithm used to compute the Assurance Token; depending on the algorithm used, one or more values may be required

Not Used C02805 1439 Assurance Token Parameter Code X ID 2/2

A code specifying the type of Assurance Token Parameter

Not Used C02806 1442 Assurance Token Parameter Value O AN 1/64

A value of a parameter, usually specifying one or more options, required for the proper operation of the cryptographic algorithm used to compute the Assurance Token; depending on the algorithm used, one or more values may be required

Not Used C02807 1439 Assurance Token Parameter Code X ID 2/2

A code specifying the type of Assurance Token Parameter

Not Used C02808 1442 Assurance Token Parameter Value O AN 1/64

A value of a parameter, usually specifying one or more options, required for the proper operation of the cryptographic algorithm used to compute the Assurance Token; depending on the algorithm used, one or more values may be required

Not Used C02809 1439 Assurance Token Parameter Code X ID 2/2

A code specifying the type of Assurance Token Parameter

Not Used C02810 1442 Assurance Token Parameter Value O AN 1/64

A value of a parameter, usually specifying one or more options, required for the proper operation of the cryptographic algorithm used to compute the Assurance Token; depending on the algorithm used, one or more values may be required

Not Used C02811 1439 Assurance Token Parameter Code X ID 2/2

A code specifying the type of Assurance Token Parameter

Not Used C02812 1442 Assurance Token Parameter Value O AN 1/64

A value of a parameter, usually specifying one or more options, required for the proper operation of the cryptographic algorithm used to compute the Assurance Token; depending on the algorithm used, one or more values may be required

Not Used C02813 1439 Assurance Token Parameter Code X ID 2/2

Not Used C02813 1439 Assurance Token Parameter Code X ID 2/2

A code specifying the type of Assurance Token Parameter

Not Used C02814 1442 Assurance Token Parameter Value O AN 1/64

A value of a parameter, usually specifying one or more options, required for the proper operation of the cryptographic algorithm used to compute the Assurance Token; depending on the algorithm used, one or more values may be required

Not Used C02815 1439 Assurance Token Parameter Code X ID 2/2

A code specifying the type of Assurance Token Parameter

Not Used	**C02816**	**1442**	**Assurance Token Parameter Value**	**O**	**AN 1/64**
			A value of a parameter, usually specifying one or more options, required for the proper operation of the cryptographic algorithm used to compute the Assurance Token; depending on the algorithm used, one or more values may be required		
Not Used	**C02817**	**1439**	**Assurance Token Parameter Code**	**X**	**ID 2/2**
			A code specifying the type of Assurance Token Parameter Refer to 003060 Data Element Dictionary for acceptable code values.		
Not Used	**C02818**	**1442**	**Assurance Token Parameter Value**	**O**	**AN 1/64**
			A value of a parameter, usually specifying one or more options, required for the proper operation of the cryptographic algorithm used to compute the Assurance Token; depending on the algorithm used, one or more values may be required		
Not Used	**C02819**	**1439**	**Assurance Token Parameter Code**	**X**	**ID 2/2**
			A code specifying the type of Assurance Token Parameter		
Not Used	**C02820**	**1442**	**Assurance Token Parameter Value**	**O**	**AN 1/64**
			A value of a parameter, usually specifying one or more options, required for the proper operation of the cryptographic algorithm used to compute the Assurance Token; depending on the algorithm used, one or more values may be required		
	S2A10	**1440**	**Assurance Digest**	**O**	**AN 1/512**
			The result of the application of the hash defined in the methodology expressed in ASCII-hex notation		

Segment: **SVA** **Security Value**

Usage: Optional

Max Use: 1

Purpose: To provide the encoded output of a cryptographic algorithm

Syntax Notes:

Semantic Notes:

Comments:

Notes: ***1. Assurance (Digital Signature) segments (S2A/SVA) are not part of the control envelope structure. When used, insert the S2A/SVA segment pair(s) immediately preceding the SE segment of the transaction set for which assurance is being provided. See Section 10.5.3 of the Federal Implementation Guidelines.***

2. The SVA segment represented here is only valid for versions 3060 and 3070.

Data Element Summary

	Ref. Des.	Data Element	Name	Attributes
Must Use	**SVA01**	**1570**	**Filter ID Code** Code specifying the type of filter used to convert data code values ASB ASCII-Baudot Filter ASC ASCII Filter HDC Hexadecimal Filter UUE Uuencoding ZZZ Mutually Defined ***Use to indicate Base 64.***	**M ID 3/3**

Must Use	**SVA02**	**799**	**Version Identifier**	**M**	**AN 1/30**

Revision level of a particular format, program, technique or algorithm

Must Use	**SVA03**	**C033**	**Security Value**	**M**	

Value of the Security Token

Must Use	**C03301**	**1572**	**Security Value Qualifier**	**M**	**ID 3/3**

Type of Security Value

ASV	Assurance Token
CRT	Certificate
	Only for use in the 3070 version of this segment.
PUB	Public Key
	Only for use in the 3070 version of this segment.

Must Use	**C03302**	**1573**	**Encoded Security Value**	**M**	**AN 1/10E16**

Encoded representation of the Security Value specified by the Security Value Qualifier

Segment: **S2E** **Security Trailer Level 2**

Usage: Optional

Max Use: 1

Purpose: To end a secured area and to provide the value of cryptographically computed authentication codes

Syntax Notes:

Semantic Notes:

Comments:

Notes: ***The S2E segment represented here is valid for versions 3040, 3050, 3060 and 3070.***

Data Element Summary

	Ref. Des.	Data Element	Name	Attributes
Must Use	**S2E01**	**997**	**Hash or Authentication Code**	**M AN 1/64**

The message authentication code or hash/digest generated by the authentication process; when the Data Encryption Standard (DES) algorithm is used, the field consists of 4 hexadecimal coded characters (i.e., characters from the set 0..9, A..F), a separator character (space, "-", or other), and 4 hexadecimally coded characters; when non-DES hashes are used, the result of the hash is expressed as hexadecimally coded characters without spaces; when authentication or hash is not used, this field should be filled with a non-blank character other than the set (0..9, A..F) for the minimum length

Enter the character "Z".

Segment: **S1A** **Assurance Level 1**

Usage: Optional

Max Use: 1

Purpose: To allow for multiple assurances at the GS/GE level

Syntax Notes:

1 If C02804 is present, then C02803 is required.

2 If C02806 is present, then C02805 is required.

3 If C02808 is present, then C02807 is required.

4 If C02810 is present, then C02809 is required.

5 If C02812 is present, then C02811 is required.

6 If C02814 is present, then C02813 is required.

7 If C02816 is present, then C02815 is required.

8 If C02818 is present, then C02817 is required.

9 If C02820 is present, then C02819 is required.

Semantic Notes:

Comments:

1 X9 has a required minimum length of four characters for S1A04 (security originator). No mechanism, or registration method, is provided by X9 or X12 to guarantee uniqueness of the identifier.

2 X9 has a required minimum length of four characters for S1A05 (security recipient). No mechanism, or registration method, is provided by X9 or X12 to guarantee uniqueness of the identifier.

3 The date/time stamp may determine which of several key values apply, depending on start and expiration dates of different key values that may share the same keyname.

4 Key distribution is performed by other means and thus only onetime keys are allowed in S1A09.

The use of particular codes and corresponding values in S1A09 is dependent on the exigencies of the various cryptographic algorithms.

Notes: ***1. Assurance (Digital Signature) segments (S1A/SVA) are not part of the control envelope structure. When used, insert the S1A/SVA segment pair(s) immediately preceding the GE segment of the group for which assurance is being provided. See Section 10.5.3 of the Federal Implementation Guidelines.***

2. The S1A segment represented here is only valid for versions 3060 and 3070..

Data Element Summary

	Ref. Des.	Data Element	Name	Attributes
Must Use	**S1A01**	**1432**	**Business Purpose of Assurance** The stated business purpose for appending the assurance to an existing secured-entity (whether functional group or transaction set); the codes represent the intention of the business or application that has control over the assurance originator ASG — Authorization Signature Appropriate to this Document CSG — Authorization Co-signature Appropriate to this Document	**M ID 3/3**
Must Use	**S1A02**	**C034**	**Computation Methods** Algorithms used to calculate an assurance	**M**
Must Use	**C03401**	**1574**	**Assurance Algorithm** Code specifying the algorithm used to compute the assurance token DSS — Digital Signature Standard ***As specified in FIPS 186.*** RSA — RSA	**M ID 3/3**
Must Use	**C03402**	**1575**	**Hashing Algorithm** Code specifying the algorithm used to compute the assurance digest	**M ID 3/3**

			MD5	MD5		
			SHA	Secure hash algorithm		
Must Use	**S1A03**	**1434**	**Domain of Computation of Assurance Digest**		**M**	**ID 1/2**

The bounds of the text, whether contiguous or not, over which the computation of the Assurance Token is computed using the defined methodology of computation and any relevant Assurance Token parameters; the "body" is either a transaction set (beginning with the ST and including all segments up to the first S2A segment, but excluding any S2S segment) or functional group (beginning with the GS and including all transaction sets up to the first S1A segment, but excluding any S1S segment

"This Assurance" is defined as from the "S" in S1A or S2A up to and including the data element separator preceeding the assurance digest

"Previous Assurance(s)" is defined as including the entire S1A or S2A segment and the entire SVA that follows the included S1A or S2A

Refer to 003060 or 003070 Data Element Dictionary, as applicable, for acceptable code values.

	S1A04	**1435**	**Assurance Originator**	**O**	**AN 1/64**

Unique designation (identity) of the cryptographic process that performs the stated assurance on data to be interchanged

Note: X9 has a required minimum length of 4 characters for a security originator; no mechanism, or registration method, is provided by X9 or X12 to guarantee uniqueness of the identifier

	S1A05	**1436**	**Assurance Recipient**	**O**	**AN 1/64**

Unique designation (identity) of the cryptographic process that performs validation of the stated assurance on received data. In the absence of an Assurance Recipient all potential receivers will often be able to validate the assurance because the cryptographic technique is based on a "public" (as opposed to "secret") technology

Note: X9 has required minimum length of 4 characters for a security recipient; no mechanism, or registration method, is pro-

vided by X9 or X12 to guarantee uniqueness of the identifier

S1A06 1443 Assurance Reference Number O AN 1/35

Alphanumeric reference number issued by security assurance originator for the particular assurance in which it occurs; unique when used in combination with security originator data element

S1A07 1437 Date/Time Reference O AN 17/25

Date/time stamp in format as follows:

YYYYMMDDHHNNSSTTTZZZ+XXXX, where YYYY = 4 digit year (with leading century), MM = month of year (01..12), DD = day of month (01..31), HH = hour of day in 24-hour format (00..23), NN = minutes of the hour (00-59), SS = second of hour (00..59), TTT = [optional] milli-seconds (000..999), ZZZ = [optional] three character, nominal time zone indicator (including daylight savings time indicator) and XXXXX = 3-5 digit (including leading + or - sign) offset of time to universal time, with three position format indicating hours-offset for whole hours, and five position format indicating hours and minutes offset where this is necessary. For example:

199306152213300CDT+0930 which represents 15 June 1993, 22:13 (10:13pm), Central Daylight Time (Nominal Value "CDT"), in a timezone that is offset + 9:30 from Universal Time (Australia)

S1A08 1438 Assurance Text O AN 1/64

Any text needed to convey the name of a signatory, registration number, certification number, or other assurance-originator defined or mutually-agreed business text related to the specific assurance; this text is not defined for X12 purposes and thus functions technically as "free form text" though it may have structure that is defined by the assurance originator, an industry group, a governmental agency, or bi-laterally between assurance originator and assurance recipient

S1A09 C028 Assurance Token Parameters O

Parameters needed to calculate the Assurance Token

Must Use C02801 1439 Assurance Token Parameter Code M ID 2/2

A code specifying the type of Assurance Token Parameter

CI	Certification Authority ID
EK	Key Value - One-Time Key
KN	Key Name
NT	Notarization
OD	Key-Encrypting-Key for One-Time Key
UI	User ID

Must Use C02802 1442 Assurance Token Parameter Value M AN 1/64

A value of a parameter, usually specifying one or more options, required for the proper operation of the cryptographic algorithm used to compute the Assurance Token; depending on the algorithm used, one or more values may be required

Not Used C02803 1439 Assurance Token Parameter Code X ID 2/2

A code specifying the type of Assurance Token Parameter

Not Used C02804 1442 Assurance Token Parameter Value O AN 1/64

A value of a parameter, usually specifying one or more options, required for the proper operation of the cryptographic algorithm used to compute the Assurance Token; depending on the algorithm used, one or more values may be required

Not Used C02805 1439 Assurance Token Parameter Code X ID 2/2

A code specifying the type of Assurance Token Parameter

Not Used C02806 1442 Assurance Token Parameter Value O AN 1/64

A value of a parameter, usually specifying one or more options, required for the proper operation of the cryptographic algorithm used to compute the Assurance Token; depending on the algorithm used, one or more values may be required

Not Used	**C02807**	**1439**	**Assurance Token Parameter Code**	**X**	**ID 2/2**
			A code specifying the type of Assurance Token Parameter		
Not Used	**C02808**	**1442**	**Assurance Token Parameter Value**	**O**	**AN 1/64**
			A value of a parameter, usually specifying one or more options, required for the proper operation of the cryptographic algorithm used to compute the Assurance Token; depending on the algorithm used, one or more values may be required		
Not Used	**C02809**	**1439**	**Assurance Token Parameter Code**	**X**	**ID 2/2**
			A code specifying the type of Assurance Token Parameter		
Not Used	**C02810**	**1442**	**Assurance Token Parameter Value**	**O**	**AN 1/64**
			A value of a parameter, usually specifying one or more options, required for the proper operation of the cryptographic algorithm used to compute the Assurance Token; depending on the algorithm used, one or more values may be required		
Not Used	**C02811**	**1439**	**Assurance Token Parameter Code**	**X**	**ID 2/2**
			A code specifying the type of Assurance Token Parameter		
Not Used	**C02812**	**1442**	**Assurance Token Parameter Value**	**O**	**AN 1/64**
			A value of a parameter, usually specifying one or more options, required for the proper operation of the cryptographic algorithm used to compute the Assurance Token; depending on the algorithm used, one or more values may be required		
Not Used	**C02813**	**1439**	**Assurance Token Parameter Code**	**X**	**ID 2/2**
			A code specifying the type of Assurance Token Parameter		
Not Used	**C02814**	**1442**	**Assurance Token Parameter Value**	**O**	**AN 1/64**
			A value of a parameter, usually specifying one or more options, required for the proper operation of the cryptographic algorithm used to compute the Assurance Token; depending on the algorithm used, one or more values may be required		
Not Used	**C02815**	**1439**	**Assurance Token Parameter Code**	**X**	**ID 2/2**
			A code specifying the type of Assurance Token Parameter		

Not Used	**C02816**	**1442**	**Assurance Token Parameter Value**	**O**	**AN 1/64**
			A value of a parameter, usually specifying one or more options, required for the proper operation of the cryptographic algorithm used to compute the Assurance Token; depending on the algorithm used, one or more values may be required		
Not Used	**C02817**	**1439**	**Assurance Token Parameter Code**	**X**	**ID 2/2**
			A code specifying the type of Assurance Token Parameter		
Not Used	**C02818**	**1442**	**Assurance Token Parameter Value**	**O**	**AN 1/64**
			A value of a parameter, usually specifying one or more options, required for the proper operation of the cryptographic algorithm used to compute the Assurance Token; depending on the algorithm used, one or more values may be required		
Not Used	**C02819**	**1439**	**Assurance Token Parameter Code**	**X**	**ID 2/2**
			A code specifying the type of Assurance Token Parameter		
Not Used	**C02820**	**1442**	**Assurance Token Parameter Value**	**O**	**AN 1/64**
			A value of a parameter, usually specifying one or more options, required for the proper operation of the cryptographic algorithm used to compute the Assurance Token; depending on the algorithm used, one or more values may be required		
	S1A10	**1440**	**Assurance Digest**	**O**	**AN 1/512**
			The result of the application of the hash defined in the methodology expressed in ASCII-hex notation		

Segment: **SVA** **Security Value**

Usage: Optional

Max Use: 1

Purpose: To provide the encoded output of a cryptographic algorithm

Syntax Notes:

Semantic Notes:

Comments:

Notes: ***1. Assurance (Digital Signature) segments (S1A/SVA) are not part of the control envelope structure. When used, insert the S1A/SVA segment pair(s) immediately preceding the GE segment of the transaction set for which assurance is being provided. See Section 10.5.3 of the Federal Implementation Guidelines.***

2. The SVA segment represented here is only valid for versions 3060 and 3070.

Data Element Summary

	Ref. Des.	Data Element	Name	Attributes
Must Use	**SVA01**	**1570**	**Filter ID Code** Code specifying the type of filter used to convert data code values ASB ASCII-Baudot Filter ASC ASCII Filter HDC Hexadecimal Filter UUE Uuencoding ZZZ Mutually Defined ***Use to indicate Base 64.***	**M ID 3/3**

Must Use	**SVA02**	**799**	**Version Identifier**	**M**	**AN 1/30**

Revision level of a particular format, program, technique or algorithm

Must Use	**SVA03**	**C033**	**Security Value**	**M**	

Value of the Security Token

Must Use	**C03301**	**1572**	**Security Value Qualifier**	**M**	**ID 3/3**

Type of Security Value

ASV	Assurance Token
CRT	Certificate
	Only for use in the 3070 version of this segment.
PUB	Public Key
	Only for use in the 3070 version of this segment.

Must Use	**C03302**	**1573**	**Encoded Security Value**	**M**	**AN 1/10E16**

Encoded representation of the Security Value specified by the Security Value Qualifier

Segment: **S1E** **Security Trailer Level 1**

Usage: Optional

Max Use: 1

Purpose: To end a secured area and to provide the value of cryptographically computed authentication codes

Syntax Notes:

Semantic Notes:

Comments:

Notes: ***The S1E segment represented here is valid for versions 3040, 3050, 3060 and 3070.***

Data Element Summary

	Ref. Des.	Data Element	Name	Attributes
Must Use	**S1E01**	**997**	**Hash or Authentication Code**	**M AN 1/64**

The message authentication code or hash/digest generated by the authentication process; when the Data Encryption Standard (DES) algorithm is used, the field consists of 4 hexadecimal coded characters (i.e., characters from the set 0..9, A..F), a separator character (space, "-", or other), and 4 hexadecimally coded characters; when non-DES hashes are used, the result of the hash is expressed as hexadecimally coded characters without spaces; when authentication or hash is not used, this field should be filled with a non-blank character other than the set (0..9, A..F) for the minimum length

Enter the character "Z".

Segment: **GE** **Functional Group Trailer**

Usage: Optional

Max Use: 1

Purpose: To indicate the end of a functional group and to provide control information

Syntax Notes:

Semantic Notes: **1** The data interchange control number GE02 in this trailer must be identical to the same data element in the associated functional group header, GS06.

Comments: **1** The use of identical data interchange control numbers in the associated functional group header and trailer is designed to maximize functional group integrity. The control number is the same as that used in the corresponding header.

Data Element Summary

	Ref. Des.	Data Element	Name	Attributes
Must Use	**GE01**	**97**	**Number of Transaction Sets Included** Total number of transaction sets included in the functional group or interchange (transmission) group terminated by the trailer containing this data element ***1. Use to identify the number of ST segments (transactions) within a functional group.*** ***2. Transmit the required number of characters without leading or trailing blanks.***	**M N0 1/6**
Must Use	**GE02**	**28**	**Group Control Number** Assigned number originated and maintained by the sender ***Cite the same group control number as was assigned by the originator in GS06.***	**M N0 1/9**

Segment: **IEA** **Interchange Control Trailer**

Usage: Optional

Max Use: 1

Purpose: To define the end of an interchange of zero or more functional groups and interchange-related control segments

Syntax Notes:

Semantic Notes:

Comments:

Data Element Summary

	Ref. Des.	Data Element	Name	Attributes
Must Use	**IEA01**	**I16**	**Number of Included Functional Groups** A count of the number of functional groups included in an interchange ***1. Use to identify the number of GS segments (functional groups) within an interchange.*** ***2. Transmit the required number of characters without leading or trailing blanks.***	**M N0 1/5**
Must Use	**IEA02**	**I12**	**Interchange Control Number** A control number assigned by the interchange sender ***Cite the same nine-digit interchange control number as was assigned by the originator in ISA13.***	**M N0 9/9**

Appendix D
Points of Contact and Web Page Information

DEPARTMENT OF DEFENSE

Air Force Office of Scientific Research (AFOSR)

Chuck Chatlynne

Telephone: (202) 767-8018

E-mail Address: chuck.chatlynne@afosr.af.mil

WWW URL: http://web.fie.com/web/fed/afr

Army Medical Research and Material Command (AMRMC)

Jeannie Shinbur

Telephone: (301) 619-7427

E-mail Address: jeannie_shinbur@ftdetrck-ccmail.army.mil

WWW URL: http://www-usamraa.army.mil

Army Research Office (ARO)

Susan Hill

Telephone: (919) 549-4338

E-mail Address: susan@aro-emh1.army.mil

WWW URL: http://www.aro.ncren.net

Office of Naval Research (ONR)

Brad Stanford

Telephone: (703) 696-5420

E-mail Address: stanfob@onr.navy.mil

WWW URL: http://www.onr.mil

FEDERAL GOVERNMENT

Department of Education

George Wagner

Telephone: (202) 708-7811

E-mail Address: george_wagner@ed.gov

WWW URL: http://www.ed.gov

Department of Energy (DOE)

Gene Hughes

Telephone: (301) 903-5409

E-mail Address: gene.hughes@hq.doe.gov

WWW URL: http://www.doe.gov

Department of Health and Human Services (DHHS)

Cara Whitehead

Telephone: (202) 690-5731

E-mail Address: cwhitehe@os.dhhs.gov

WWW URL: http://www.os.dhhs.gov

CENTERS FOR DISEASE CONTROL (CDC)

Ron Van Duyne

Telephone: (404) 842-6517

E-mail Address: rsv0@cdc.gov

WWW URL: http://www.cdc.gov

NATIONAL INSTITUTES OF HEALTH (NIH)

Diana Jaeger

Telephone: (301) 435-0932

E-mail Address: dj12u@nih.gov

WWW URL: http://www.nih.gov

Department of Transportation (DOT)

Ann Fisher

Telephone: (202) 366-4288

E-mail Address: ann.fisher@ost.dot.gov

WWW URL: http://www.dot.gov

Financial Management Services (FMS), (Department of Treasury)

Carolyn Austin-Diggs

Telephone: (202) 874-6510

E-mail Address: carolyn.austin-diggs@fms.sprint.com

WWW URL: http://www.fms.treas.gov

National Science Foundation (NSF)

Jean Feldman

Telephone: (703) 306-1243

E-mail Address: jfeldman@nsf.gov

WWW URL: http://www.nsf.gov

United States Department of Agriculture (USDA), Cooperative State Research, Education, and Extension Service (CSREES)

Robert MacDonald, Ph.D.

Telephone: (202) 205-5967

E-mail Address: rmacdonald@reeusda.gov

WWW URL: http://www.reeusda.gov

FEDERAL DEMONSTRATION PARTNERSHIP (FDP)

Gerald B. Stuck (ERA Coordinator)

Telephone: (703) 917-7555

E-mail Address: gstuck@nsf.gov

WWW URL: http://www.dml.georgetown.edu/fdp

Appendix E
Glossaries from the Federal Implementation Guidelines for EDI

This appendix contains two glossaries taken directly from the *Federal Implementation Guidelines for Electronic Data Interchange (EDI)* prepared by the Federal Electronic Commerce Acquisition Program Management Office (ECA-PMO). The glossaries define terms specific to ASC X12 and federal government EDI. The latest and most current version of this information is available on the federal EDI home page.[1]

X12 GLOSSARY

ANSI

American National Standards Institute

ANSI Standard

A document published by ANSI that has been approved through the consensus process of public announcement and review. Each such standard must have been developed by an ANSI committee and must be revisited by that committee within 5 years for updating. See Draft Standard for Trial Use (DSTU).

ASC X12

Accredited Standards Committee, X12. It comprises government and industry members who create electronic data interchange (EDI) standards for submission to ANSI for subsequent approval and dissemination.

Authentication

A mechanism that allows the receiver of an electronic transmission to verify the sender and the integrity of the content of the transmission through the use of an electronic "key" or algorithm shared by the trading partners. That algorithm is sometimes referred to as an electronic signature.

[1]Secretariat for Federal EDI, "Federal Guidelines" (Web site), http://snad.ncsl.nist.gov/dartg/edi/guideline.html

Compliance Checking

A checking process that is used to ensure that a transmission complies with ANSI X12 syntax rules.

Conditional (C)

A data element requirement designator that indicates that the presence of a specified data element is dependent on the value or presence of other data elements in the segment. The condition must be stated and must be computer-processable.

Control Segment

A segment that has the same structure as a data segment but is used for transferring control information for grouping data segments. Control segments may be loop control segments (LS/LE), transaction set control segments (ST/SE), or functional group control segments (GS/GE), defined in X12.6, or interchange control segments (ISA/IEA/TA1), defined in X12.5.

Data Element

The basic unit of information in the EDI standards containing a set of values that represent a singular fact. It may be single-character codes, literal descriptions, or numeric values.

Data Element Length

The range, minimum to maximum, of the number of character positions available to represent the value of a data element. A data element may be of variable length and range from minimum to maximum or it may be of fixed length in which the minimum is equal to the maximum.

Data Element Reference Number

Number assigned to each data element as a unique identifier.

Data Element Requirement Designator

A code defining the need for a data element value to appear in the segment if the segment is transmitted. The X12 codes are mandatory (M), optional (O), or conditional (C). The government may consider a segment “mandatory” even through it is “optional” by X12 standards.

Data Element Separator

A unique character preceding each data element that is used to delimit data elements within a segment. Government uses “*” as the delimiter.

Data Element Type

A data element may be one of six types: numeric, decimal, identifier, string, date, or time.

Delimiters

Two levels of separators and a terminator. The delimiters are an integral part of the transferred data stream. They are specified in the interchange header and may not be used in a data element value elsewhere in the interchange. From highest to lowest level, the separators and terminators are segment terminator and data element separator.

DISA

Data Interchange Standards Association. A nonprofit organization funded by ASC X12 members to serve as the Secretariat for X12.

DISA

Defense Information Systems Agency. The Department of Defense's (DoD's) Executive Agency for all information systems technology.

DSTU

Draft Standard for Trial Use. Represents a document approved for publication by the full X12 committee following membership consensus and subsequent resolution of negative votes. (Final Report of X12 Publications Task Group). The Draft EDI Standard for Trial Use document represents an ASC X12 approved standard for use prior to approval by ANSI. See ANSI Standard.

EDI

Electronic data interchange. The computer-application-to-computer-application exchange of business information in a standard format.

Electronic Commerce

Electronic Commerce is the integration of electronic mail, electronic funds transfer, EDI, and similar techniques into a comprehensive, electronic-based system encompassing all business functions, including procurement, payment, supply management, transportation, and base operations.

Electronic Envelope

Electronic information that binds together a set of transmitted documents being sent from one sender to one receiver.

Element Delimiter

A single-character that follows the segment identifier and separates each data element in a segment except the last.

Functional Group

A group of one or more transaction sets bounded by a functional group header segment and a functional group trailer segment.

Functional Group Segments (GS/GE)

These segments identify a specific functional group of documents such as purchase orders.

Industry Conventions

Defines how the ASC X12 standards are used by the specific industry.

Industry Guidelines

Defines the EDI environment for using conventions within an industry. It provides assistance on how to implement X12 standards.

Interchange Control Segments (ISA/IEA)

These segments identify a unique interchange being sent from one sender to one receiver (see electronic envelope).

Interchange Control Structure

The interchange header and trailer segments that envelop one or more functional groups or interchange-related control segments and perform the following functions: (1) define the data element separators and the data segment terminators, (2) identify the sender and receiver, (3) provide control information for the interchange, and (4) allow for authorization and security information. (X12.5)

Loop

A group of semantically related segments; these segments may be either bounded or unbounded (X12.6). The N1 loop is an example of a loop, which includes Segments N1 to PER for name and address information.

Mandatory (M)

A data element/segment requirement designator that indicates the presence of a specified data element is required.

Mapping

The process of identifying the standard data element's relationship to application data elements.

Max Use

Specifies the maximum number of times a segment can be used at the location in a transaction set.

Message

Entire data stream including the outer envelope.

Optional (O)

A data element/segment requirement designator that indicates the presence of a specified data element/segment is at the option of the sending party and can be based on the mutual agreement of the interchange parties.

Qualifier

A data element that identifies or defines a related element, set of elements, or a segment. The qualifier contains a code taken from a list of approved codes.

Repeating Segment

A segment that may be used more than once at a given location in a transaction set. See Max Use.

Security

System screening that denies access to unauthorized users and protects data from unauthorized uses.

Segment

Segments consist of logically related data elements in a defined sequence. A data segment consists of a segment identifier, one or more data elements each preceded by an element separator, and a segment terminator.

Segment Directory

Provides the purpose and format of the segments used in the construction of transaction sets. The directory lists each segment by name, purpose, identifier, the contained data elements in the specified order, and the requirement designator for each data element.

Segment Identifier

A unique identifier for a segment, consisting of a combination of two or three upper-case letters and digits. The segment identifier occupies the first-character positions of the segment. It is not a data element.

Segment Terminator

A unique character appearing at the end of a segment to indicate the termination of the segment, e.g., N/L.

Syntax

The grammar or rules that define the structure of the EDI standards (i.e., the use of loops, qualifiers, etc.). Syntax rules are published in ANSI X12.6.

Transaction Set

A document that unambiguously defines, in the standard syntax, information of business or strategic significance and consists of a header segment, one or more data segments in a specified order, and a trailer segment.

Transaction Set Area

A predefined area within a transaction set (header, detail, summary) containing segments and their various attributes.

Transaction Set ID

An identifier that uniquely identifies the transaction set. This identifier is the first data element of the transaction set header segment.

Translation

The act of accepting documents in other than standard format and translating them to the standard.

Version/Release

Identifies the publication of the standard being used for the generation or the interpretation of data in the X12 standard format. May be found in the Functional Group Header Segment (GS) and in the Interchange Control Header Segment (ISA). See Control Segment.

X12

The ANSI committee responsible for the development and maintenance of standards for EDI.

X12.5

Interchange Control Structure. This standard provides the interchange envelope of a header and trailer for the electronic interchange through a data transmission, and it provides a structure to acknowledge the receipt and processing of this envelope.

X12.6

Application Control Structure. This standard describes the control segments used to envelop loops of data segments, transaction sets, and groups of related transaction sets.

FEDERAL GLOSSARY

AIS

Automated information systems

DES

Data encryption standard

DFAS

Defense Finance and Accounting Service

DISA

Defense Information Systems Agency

DLMS

Defense Logistics Management System

ECA-PMO

Federal Electronic Commerce Acquisition Program Management Office

FMS

Financial Management Service

GSA

General Services Administration

ISA

Interchange control header identifier

NIST

National Institute of Standards and Technology

NTE

Note identifier

OFPP

Office of Federal Procurement Policy

OMB

Office of Management and Budget

PLUS

Protection of logistics unclassified/sensitive systems

SMC

Standards Management Committee

UN/EDIFACT

EDIFACT; electronic data interchange for administration, commerce, and transport