

**Preliminary
UN/EDIFACT ORDERS Message
Implementation and Test Plan**

**for the
DOD CALS IDE Project**

March 1998

In support of
Contract DASW01-97-D-0006

MANAGEMENT
TECHNOLOGY MASI
ManTech Advanced Technology Systems

Robert S. Kidwell
Vice President/Senior Technical Director
DoD CALS IDE Project

TABLE OF CONTENTS

LIST OF FIGURES	IV
LIST OF TABLES.....	V
1.0 INTRODUCTION	1
1.1 Overview and Background.....	1
1.2 Approach.....	3
2.0 ARCHITECTURE FRAMEWORK MODEL FOR TESTING	5
2.1 Layer 1: Application Interface: Outbound	8
2.2 Layer 2: Transaction Generation: Outbound.....	9
2.3 Layer 3: Network Communications: Outbound/Inbound	11
2.4 Layer 4: Transaction Interpretation: Inbound	13
2.5 Layer 5: Application Interface: Inbound	14
3.0 TEST SCHEDULE	16
3.1 Test Planning, Scheduling, and Resources	16
3.2 Government Activities	16
3.3 Test Report	16
3.4 Outreach.....	17
4.0 TEST METHODOLOGY	18
4.1 Testing Strategy.....	18
4.2 Assumptions and Constraints	18
4.3 Risk Assessment	21
4.3.1 Risk Identification and Impact	21
4.3.1.1 Communications/Network	21
4.3.1.2 Operational.....	22
4.3.1.3 Administrative	23
4.3.2 Control Objectives.....	23
4.4 Test Requirements	25
4.4.1 Basic Functions	26
4.4.2 Data Format and Content	28
4.5 Test Results Analysis and Reporting	30
4.5.1 Data Analysis	31
4.5.2 Test Documentation.....	32
5.0 FEDORDER D.97A TEST CASES.....	33
5.1 FEDORDERS D.97A Test Case Basic Information.....	33
5.1.1 Test Objective	33
5.1.2 Test Requirements.....	33
5.1.3 Software Test Environment	34
5.1.4 Hardware Test Environment.....	34
5.1.5 Installation, testing, and control.....	35
5.1.6 Data Recording and Analysis.....	35
5.2 FEDORDERS D.97A Test Case Scenarios	36
5.2.1 Scenario 1: Use ECI with translation occurring within ECI.....	36
5.2.2 Scenario 2: Use ECI with Translation Outside of ECI.....	37
5.2.3 Scenario 3: Bypass ECI with Local Translation	38

6.0 SUMMARY AND CONCLUSIONS..... 39
APPENDIX A: GLOSSARY A-1
APPENDIX B: ABBREVIATIONS AND ACRONYMS..... B-1

LIST OF FIGURES

Figure 1.2-1 UN/EDIFACT ORDERS Message Prototype Testing Approach	3
Figure 1.2-2 Business Process Requirements Assessment Methodology.....	4
Figure 2.0-1 Electronic Purchasing Testing Architecture	7
Figure 2.0-2 UN/EDIFACT ORDERS Message Prototype Test Suite Matrix	8
Figure 2.1-1 Application Interface: Outbound.....	8
Figure 2.2-1 Transaction Generation: Outbound.....	10
Figure 2.3-1 Network Communications: Outbound/Inbound.....	12
Figure 2.4-1 Transaction Interpretation: Inbound	13
Figure 2.5-1 Application Interface: Inbound	14
Figure 4.2-1 ManTech Testing Agent DataFlow	20
Figure 5.2-1 Task 3 Architecture.....	36

LIST OF TABLES

Table 2.0-1 Architectural Framework Model Areas	7
Table 3.1-1 Testing Schedule	16
Table 4.4.1-1 Basic Requirements Test Table	27
Table 4.4.2-1 Data Format and Contents Requirements Test Table	30

1.0 INTRODUCTION

This report represents the second deliverable for Task 3 (*Purchasing EDI Support*) for the Department of Defense (DoD) Integrated Data Environment (IDE) Program, which is entitled *Preliminary UN/EDIFACT ORDERS Message Prototype Strategy and Test Plan Document*. The overall goal of this task is to coordinate with the Continuous Acquisition and Life-cycle Support (CALs) Industry Steering Group (ISG) to develop a trial test of the United Nations rules for Electronic Data Interchange For Administration, Commerce and Transport (UN/EDIFACT) ORDERS message within the context of Basic Ordering Agreements (BOA) and simple delivery orders. The initial deliverable for this task (*Preliminary UN/EDIFACT ORDERS Message Assessment*) provided a general assessment of the ORDERS message's structure, syntax, and semantics, and defined both the architectural framework for testing the ORDERS message as well as the risk assessment and requirement analysis to support this testing.

The strategy for trial testing the UN/EDIFACT ORDERS message in actual "live" business environments with coordination from the CALS ISG, Government, and industry will be developed into a test plan, which is the basis for this report. This testing process will involve a mock test of the ORDERS message, as it would be transmitted from Government to trading partners. Upon finishing the test, a test analysis report will be prepared, which will document findings, conclusions, and recommendations resulting from the test and will be entitled the *ORDERS Message Prototype Test Report*. This analysis report will be disseminated to both participants in the Federal X12 Electronic Commerce/Electronic Data Interchange (EC/EDI) Program and interested industry members. The two additional reports following the test report include a strategy document for reaching out to industry and informing companies of migration plans for EDIFACT and an information package supporting the outreach strategy. Because it is important to understand what necessitated the development UN/EDIFACT ORDERS message prototype and testing of this prototype in the DoD, the following section is provided.

1.1 Overview and Background

The President via Executive Order has initiated a major program to improve federal purchasing through the use of EDI technology. In response to this initiative, federal agencies have begun to build upon industry successes with United States X12 EDI standards and to use electronic techniques to accomplish smaller Government procurements (e.g., purchase orders, request for quotes, quotes, etc.). Concurrent with these activities, several larger U.S. firms are expressing interest in accelerating migration to United Nations EDIFACT standards for international data interchange. The United States has committed to a process alignment between the domestic American National Standards Institute (ANSI) X12 EDI standard, and the international UN/EDIFACT standard. The EDIFACT standards are primarily used in Europe and Asia. However, in order for everyone to benefit from a single global EDI standard, ANSI X12 has agreed to begin a gradual alignment with EDIFACT in 1997. The ANSI X12 alignment plan includes for administrative alignment and technical migration to UN/EDIFACT. As a result of this migration and the growing acceptance of UN/EDIFACT standards within Europe, Japan, South Korea, the North Atlantic Treaty Organization (NATO), Australia and other countries,

representatives of the DoD and federal procurement organizations have intensified efforts to migrate business functionality pertaining to purchase orders to EDIFACT.

An EDIFACT Industry Analysis was performed by ManTech to aid the DoD in developing a point of view regarding migration to the UN/EDIFACT standard. Various U.S. industries and industry associations were surveyed to gather their thoughts on where U.S. industries were heading in regards to the UN/EDIFACT standard. Participants were asked five core questions.

1. Within the U.S., both industry and Government are expressing interest in accelerating migration to and alignment with UN/EDIFACT standards for EDI. In your opinion, from the perspective of an EDI professional, do you feel that your industry as a whole has committed to this alignment and are productively moving towards it?
2. Are you currently using the UN/EDIFACT standard?
3. If UN/EDIFACT is currently in use, what was the driving reason for the implementation of UN/EDIFACT over X12?
4. If UN/EDIFACT is not currently being used, has there been discussion within your company of migration to the UN/EDIFACT standard? If so, what is your timeframe for completing the implementation and what are the driving forces behind this migration?
5. Due to fundamental differences between the two standards, ANSI X12 and UN/EDIFACT, do you foresee a serious 'push' to reach this alignment among those companies that are currently EDI capable?

Fifteen specific industries were targeted: Automotive, Aviation, Banking and Finance, Communications, Consulting, Electronics, Energy and Utilities, Healthcare, Insurance, Petroleum, Publishing, Raw Materials, Retail, Software, and Transportation. Most large companies that traded internationally conveyed that they use the EDIFACT standards due to their international business and do see a slow progress toward EDIFACT use within the U.S. Some companies such as Texas Instruments Semi-Conductors and General Motors are focused on the implementation of UN/EDIFACT standards. These large firms are in turn requiring smaller business partners to broaden their EDI capabilities to encompass EDIFACT standards. Most U.S. industries dealing with international trade are beginning to incorporate UN/EDIFACT into their EDI systems, however there does not appear to be major moves, outside of large firms such as General Motors, towards EDIFACT for use within the domestic U.S. marketplace. It appears that it is easier at this time for companies to support both standards than to expend a great deal of effort migrating from one standard to the other especially while they are contending with Y2K issues. Since the U.S. Government deals with international trade, on some level UN/EDIFACT will need to be incorporated into its EDI capabilities.

The business functionality of both the DoD and federal procurement organization's *purchase orders* process will therefore be trial tested using a prototype implementation of the UN/EDIFACT ORDERS message. The specific objective of this task is to test the ORDERS message in coordination with the DoD Electronic Commerce Infrastructure (ECI) architecture within the context of basic ordering agreements and simple delivery orders. This report provides the test plan for administering and reporting of all testing. The following section explains how we plan to approach this task.

1.2 Approach

A prevailing concern in approaching this task is the uncertain final form of the UN/EDIFACT ORDERS message. The U.S. DoD has been working through the Pan American EDIFACT Board to augment the ORDERS message in order to satisfy DoD requirements. A draft release of FEDORDER D.97A was released August 15, 1997. The general approach for accomplishing the overall task is presented in Figure 1.2-1.

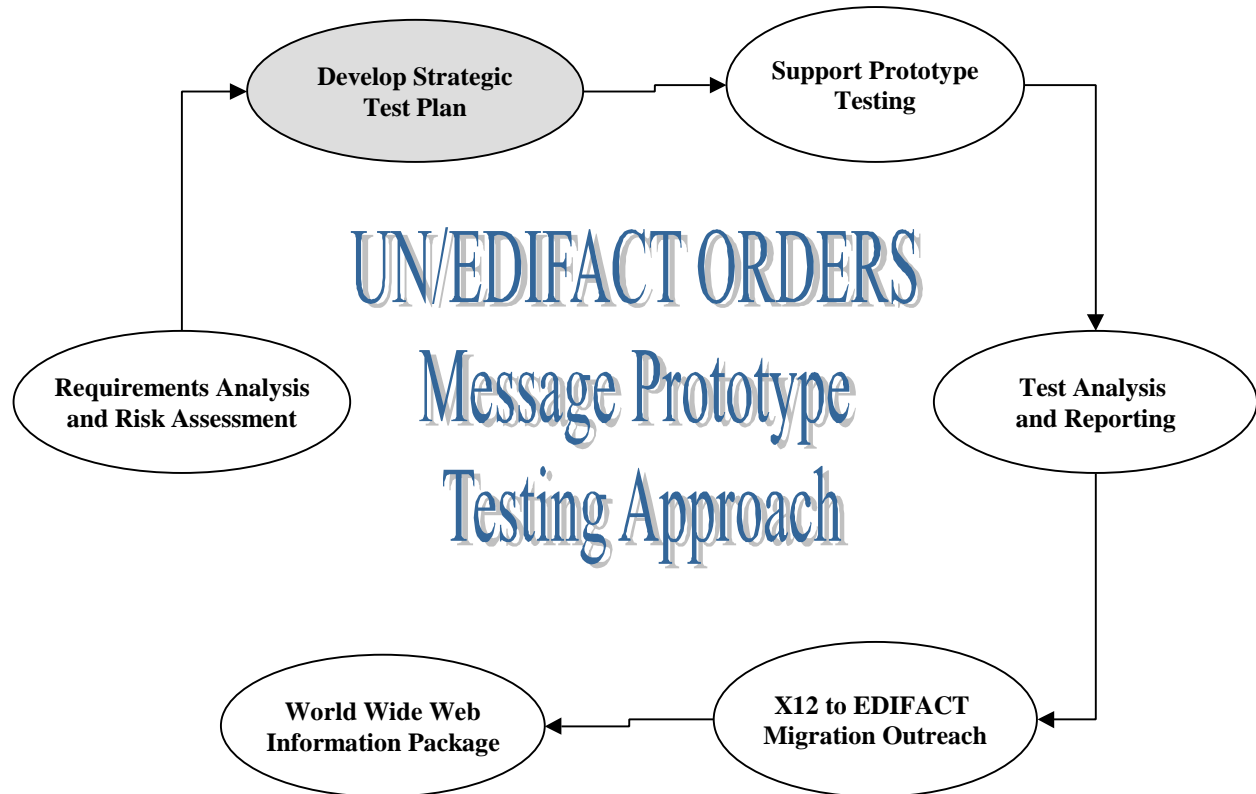


Figure 1.2-1 UN/EDIFACT ORDERS Message Prototype Testing Approach

Because testing of the ORDERS message involves many areas of complexity, a well defined and organized understanding of the ORDERS message and EC/EDI systems area must be embodied in our test plan. The ORDERS message basically specifies details for goods or services ordered using EDI between trading partners involved in administration, commerce, and transport under conditions agreed between the seller and the buyer. When considering requirements relating to the basic ordering or simple delivery order business process it is important to understand what is implied by a BOA or a simple delivery order. Requirements for the BOA business process will be identified as illustrated in Figure 1.2-2.

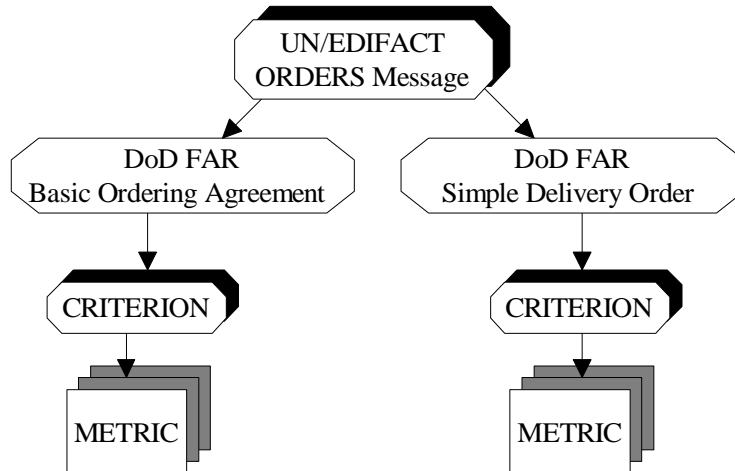


Figure 1.2-2 Business Process Requirements Assessment Methodology

A BOA is an instrument of understanding (not a contract) executed between a procuring activity and a contractor which sets forth negotiated contract clauses which will be applicable to future procurements entered into between the parties during the term of the agreement. It includes as specific as possible a description of the supplies or services and a description of the method for determination of prices.

Our approach for developing a plan for testing the prototype ORDERS message, in coordination with the CALS ISG, Government, and industry, will follow the steps outlined below.

- Describe test plan and objective.
- Plan, schedule, and allocate resources for testing.
- Identify, define, and agree on test requirements.
- Define verdict criteria.
- Formulate test strategy.
- Identify and define test process and procedures.
- Define consistent technique for reporting the test results.

2.0 ARCHITECTURE FRAMEWORK MODEL FOR TESTING

Before developing a test plan for testing the prototype ORDERS message, sufficient structure and clarity must be built into the process of developing and implementing the actual tests. All testable physical and functional components in this framework will therefore be identified and defined in this section. Before going into a detailed discussion of the functional aspects of the testing framework, it is necessary to briefly describe the physical product areas within this architecture. These product areas include the following:

Product Areas:

1. Application Interface
2. Data
3. Communications/Network
4. Off-The-Shelf Software

Within these 4 product areas, there are 17 specific products that may be tested. Each product area is defined in this section.

The first product area, *Application Interface*, simply refers to the software programs that either generate or receive relevant data for or from the EC/EDI transaction. Individual products identified in this category include:

Application Interfaces:

1. Government Automated Information System (AIS) - EC/EDI System.
2. Business Application - EC/EDI System.

The second product area, *Data*, simply refers to the various data sets that are encountered in the EC/EDI process. Individual data products identified in this category include:

Data:

1. Data exported from the Government AIS.
2. EC/EDI translation process output data.
3. Data exported as a User Defined Format (UDF).

The third product area, *Communications*, simply refers to the hardware, software, and networking components necessary for transporting EC/EDI messages to and from trading partners. Individual products identified in this category include:

Communications/Network:

1. Government Gateway
2. Electronic Commerce Processing Node (ECPN)
3. N-level Internet Protocol Router Network (NIPRnet) - Internet Bridge
4. Value Added Network (VAN)
5. Leased Line connection

The fourth product area, *Off-The-Shelf Software*, simply refers to the various data sets that are encountered in the EC/EDI process. Individual off-the-shelf software products identified in this category might include:

Off-The-Shelf Software:

1. Translation and Mapping
2. Database
3. Communications
4. EDI Mailbox
5. Security
6. Audit Logging
7. Archival and Restoration

When considering testing any system, it is meaningful to not only examine the system as a whole, but to also examine individual test areas that make up the system. A functional decomposition of the EC/EDI process has therefore been performed and architecture documented. This EC/EDI testing architecture demonstrates the functions that apply to all EC/EDI systems, regardless of what transaction sets or messages are being exchanged. This architecture for testing allows for requirements to be partitioned into self-contained areas of functionality and will serve as the foundation for developing a modular test plan. It should be noted that streamlining of the testing process will be facilitated using a qualification process as described in Section 4.0 of this report.

The primary objective of this model is to put in place a structure on which the test plan may be developed. This model provides a framework that will be used to reference the various levels of testing involved in testing EC/EDI systems for conformance to relevant DoD requirements. To this end, a five-layered model depicting the distinct and separate levels at which testing may occur, hereinafter referred to as the “*Architectural Framework Model for Testing EC/EDI Systems*,” was developed. This model will be used as a reference guide for developing and implementing the individual EC/EDI test sets in accordance with this task.

A preliminary study of the electronic purchasing process reveals a functionally symmetrical testing architecture involving both automated business transactions and data translations that are centered around network telecommunications through which this data is transmitted between DoD and industry trading partners. The data flow for this process is bi-directional (inbound vs. outbound) as illustrated in Figure 2.0-1.

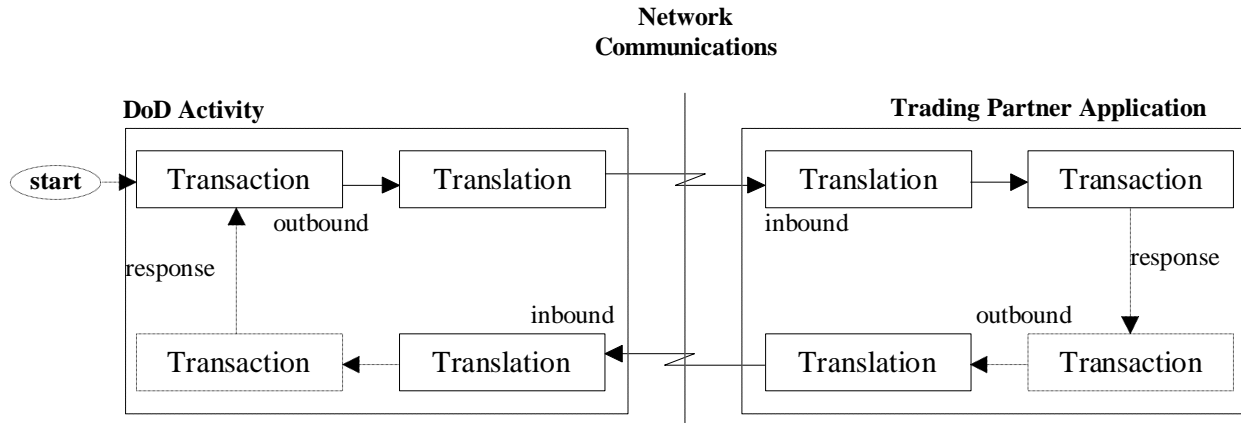


Figure 2.0-1 Electronic Purchasing Testing Architecture

Table 2.0-1 summarizes the model areas and lists some characteristic areas that may be targeted for testing for each area.

Table 2.0-1 Architectural Framework Model Areas

Architecture Model Areas		Testable Aspects
1	Transaction	Transaction Syntax and Semantics, and Conformance to the Implementation Conventions, Implementation Guidelines (Trading Partner Agreements).
2	Translation	Translation Syntax and Semantics, Error Handling, Performance Time, Authentication, Security, Bounds Testing (reasonability test).
3	Network Communications	Transmission/Reception Performance Time, Reliability, Response Time, Authentication, Security, Data Retention.

When considering the interface between the EC/EDI transaction/translation systems and the application programs (i.e., order processing, purchase order generation, accounts payable, accounts receivable, etc.) the testing architecture is augmented to include two additional layers (Layer 1, Layer 5) as follows:

- Layer 1: Application Interface: Outbound
- Layer 2: Transaction Generation: Outbound
- Layer 3: Network Communications: Outbound/Inbound
- Layer 4: Transaction Interpretation: Inbound
- Layer 5: Application Interface: Inbound

A matrix comparison of these functional layers of the architectural framework model and the EC/EDI product areas were used to identify independent self-contained areas of functionality (which is the basis for identifying test sets as illustrated in Figure 2.0-2).

	Application Interface	Data	Network / Communication	Off-The-Shelf Software
Layer 1	AIO-AI Test Set(s)	AIO Data Test Set(s)		AIO Software Test Set(s)
Layer 2		TG Data Test Set(s)		TG Software Test Set(s)
Layer 3		N/C Data Test Set(s)	N/C N/C Test Set(s)	N/C Software Test Set(s)
Layer 4		TI Data Test Set(s)		TI Software Test Set(s)
Layer 5	AII-AI Test Set(s)	AII Data Test Set(s)		AII Software Test Set(s)

Figure 2.0-2 UN/EDIFACT ORDERS Message Prototype Test Suite Matrix

All test sets and specific test cases will be subsequently designed and implemented atop this foundation. Figure 2.0-2 reveals 13 test sets for the UN/EDIFACT ORDERS Message Prototype Test Suite. Sections 2.1 through 2.5 examine the individual layers of the test architecture and provide flow diagrams for each layer of functionality defined.

2.1 Layer 1: Application Interface: Outbound

The outbound application interface layer represents the interface between the Government AIS and their EDI translation/transaction application. Transactions are entered via the AIS, data is extracted and mapped to a UDF readable format, and then presented to the translator as illustrated in Figure 2.1-1.

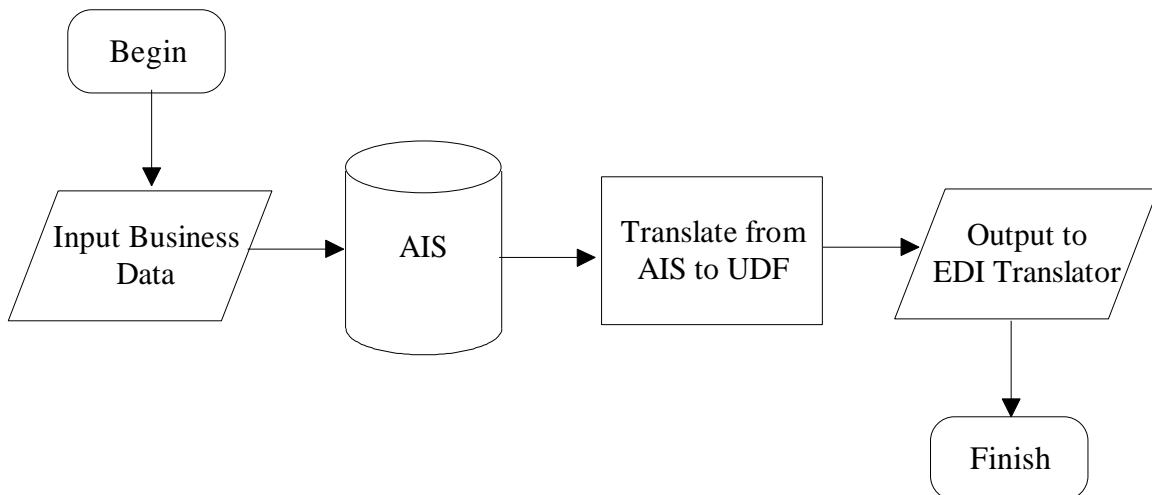


Figure 2.1-1 Application Interface: Outbound

In summary, the three functional areas for this layer include:

1. Input/editing of business data (i.e., purchase order).
2. Perform business data translation from AIS to UDF.
3. Present business data to EDI translator.

Preliminary analysis of the test suite matrix reveals the following three test sets for Layer 1 of the testing model:

1. Application Interface: Outbound - Application Interface Test Set.
2. Application Interface: Outbound - Data Test Set.
3. Application Interface: Outbound - Software Test Set.

2.2 Layer 2: Transaction Generation: Outbound

The outbound transaction generation layer involves reading and processing the EDI transaction data for formatting and transmission of the EDI message from the Government entity to the communications system. The functional steps involved in this layer are illustrated in Figure 2.2-1.

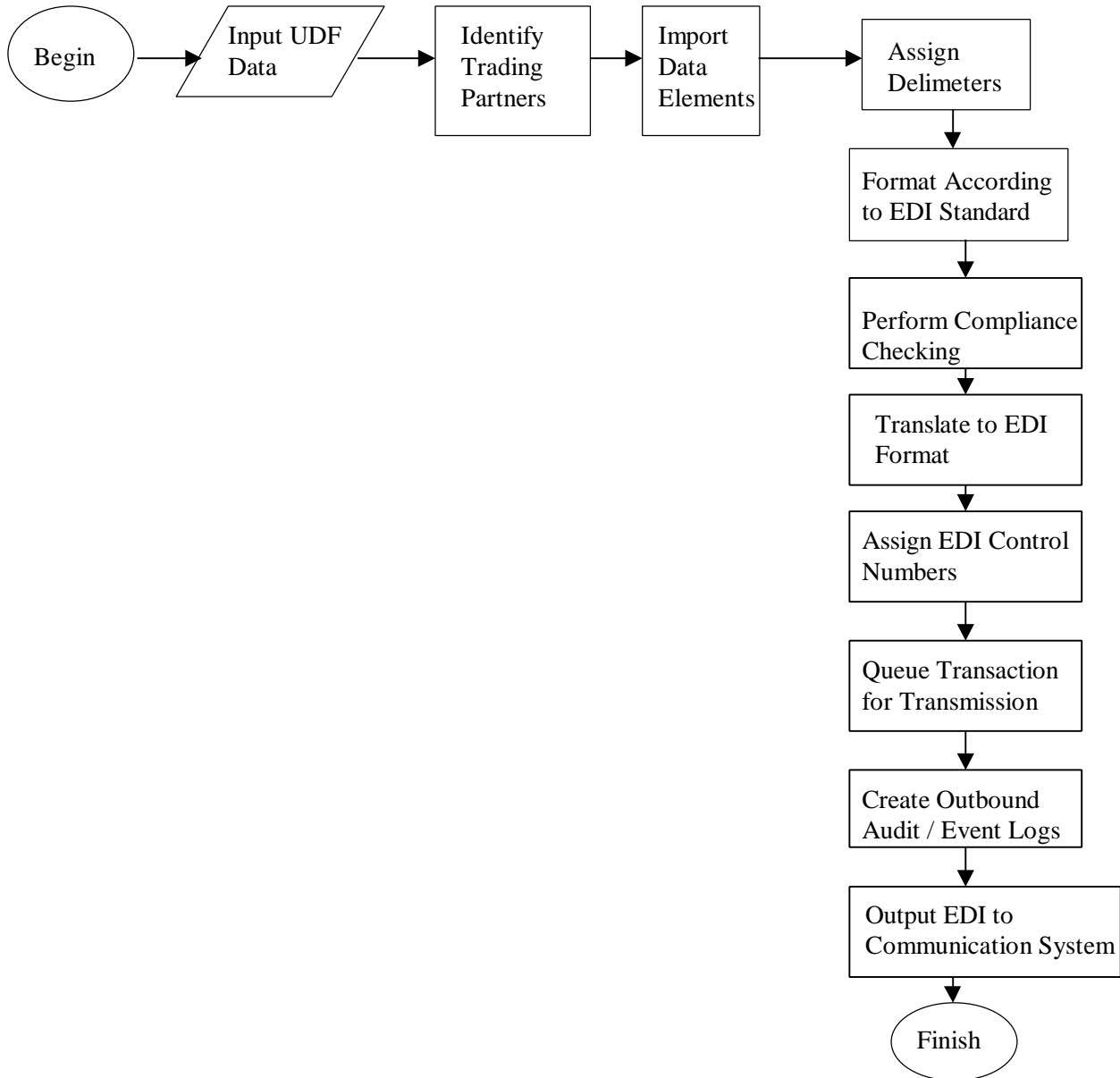


Figure 2.2-1 Transaction Generation: Outbound

In summary, the functional areas for this layer include:

1. Input/editing of business data (i.e., purchase order).
2. Identify trading partners.
 - Identify sender / receiver Ids.
 - Identify Implementation Conventions (IC).
3. Present business data to EDI translator.
 - Import data elements.
 - Assign data delimiters.

- Perform data transformation from UDF to ANSI X12 or EDIFACT standard compliant format.
- Perform EDI compliance checking:
 - Check that mandatory fields contain data (e.g., date and invoice number).
 - Check that the optional and conditional requirements of the data are satisfied.
 - Check for correct data types in fields (i.e., alphabetic, alphanumeric, numeric).
 - Check data sequence by element, segment, transaction set/message, and by batch.
- 4. Assign EDI control numbers.
- 5. Queue transactions for transmission.
- 6. Create audit/event/error logs.
- 7. Present EDI interchange data to communication system handler.

Preliminary analysis of the test suite matrix reveals the following two test sets for Layer 2 of the testing model:

1. Transaction Generation: Outbound - Data Test Set.
2. Transaction Generation: Outbound - Software Test Set.

2.3 Layer 3: Network Communications: Outbound/Inbound

The communications layer represents the hardware, software, and networks within ECI for Government and industry to interchange EC/EDI information. The primary function of this layer is to interface the ECPNs with the industry VANs. The functional steps involved in this layer are illustrated in Figure 2.3-1.

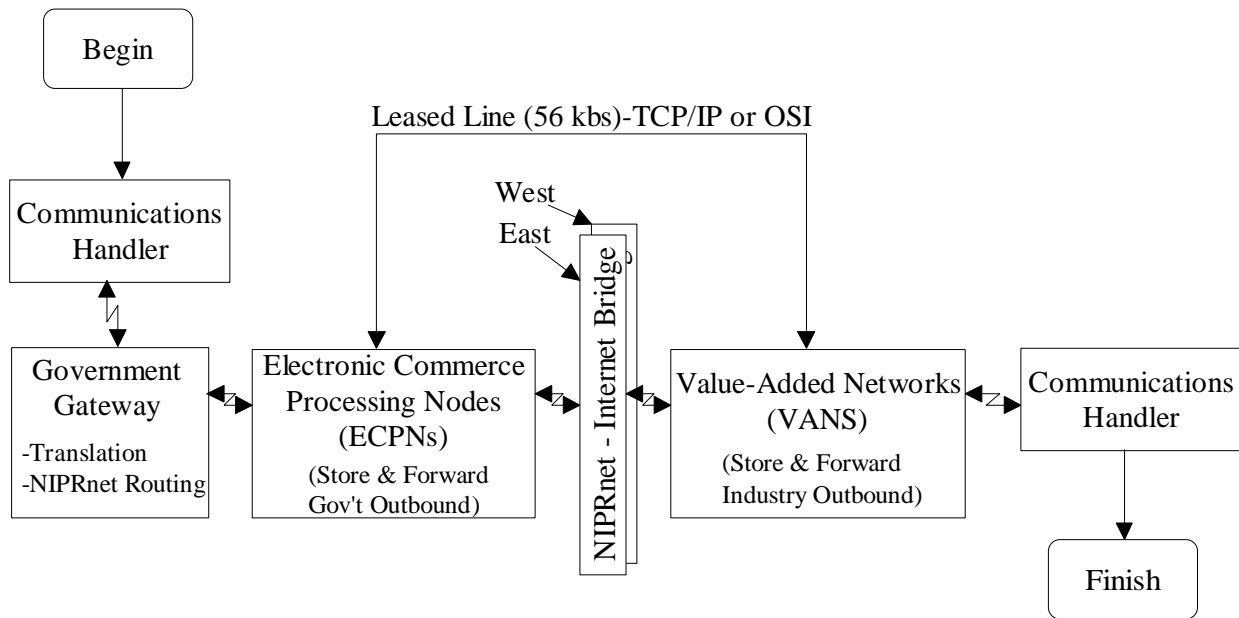


Figure 2.3-1 Network Communications: Outbound/Inbound

It is important to note that within this communications architecture the ECPN is connected to the VAN by either the leased line or the Internet - NIPRnet Bridge. In either event, the same protocols are used for transmission and communications of data.

In summary, the five primary functional areas for this layer include:

1. Establish Communications Link
 - Access Security
 - Authenticate
2. Protocol Support
 - Transmission Control Protocol /Internet Protocol (TCP/IP) [File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP)]
 - Open Systems Interconnection (OSI) (X.400, X.435)
3. Receive Transaction (inbound)
 - Decryption
 - Receive EDI Message
4. Store Transaction
 - Create/maintain Audit Logs
 - Archiving
 - Retransmission
5. Forward Transaction
 - Encryption
 - Transmit EDI Message
 - Route to Trading Partner

Preliminary analysis of the test suite matrix reveals the following three test sets for Layer 3 of the testing model:

1. Network Communications - Data Test Set.
2. Network Communications - Network Communications Test Set.
3. Network Communications - Software Test Set.

Because Layer 3 involves data both being transmitted outbound and data being received inbound, consideration to the direction of data flow will be reflected in the development of Layer 3 test sets.

2.4 Layer 4: Transaction Interpretation: Inbound

The inbound transaction interpretation layer involves reading and processing the EDI formatted transaction data. The functional steps involved in this layer are illustrated in Figure 2.4-1.

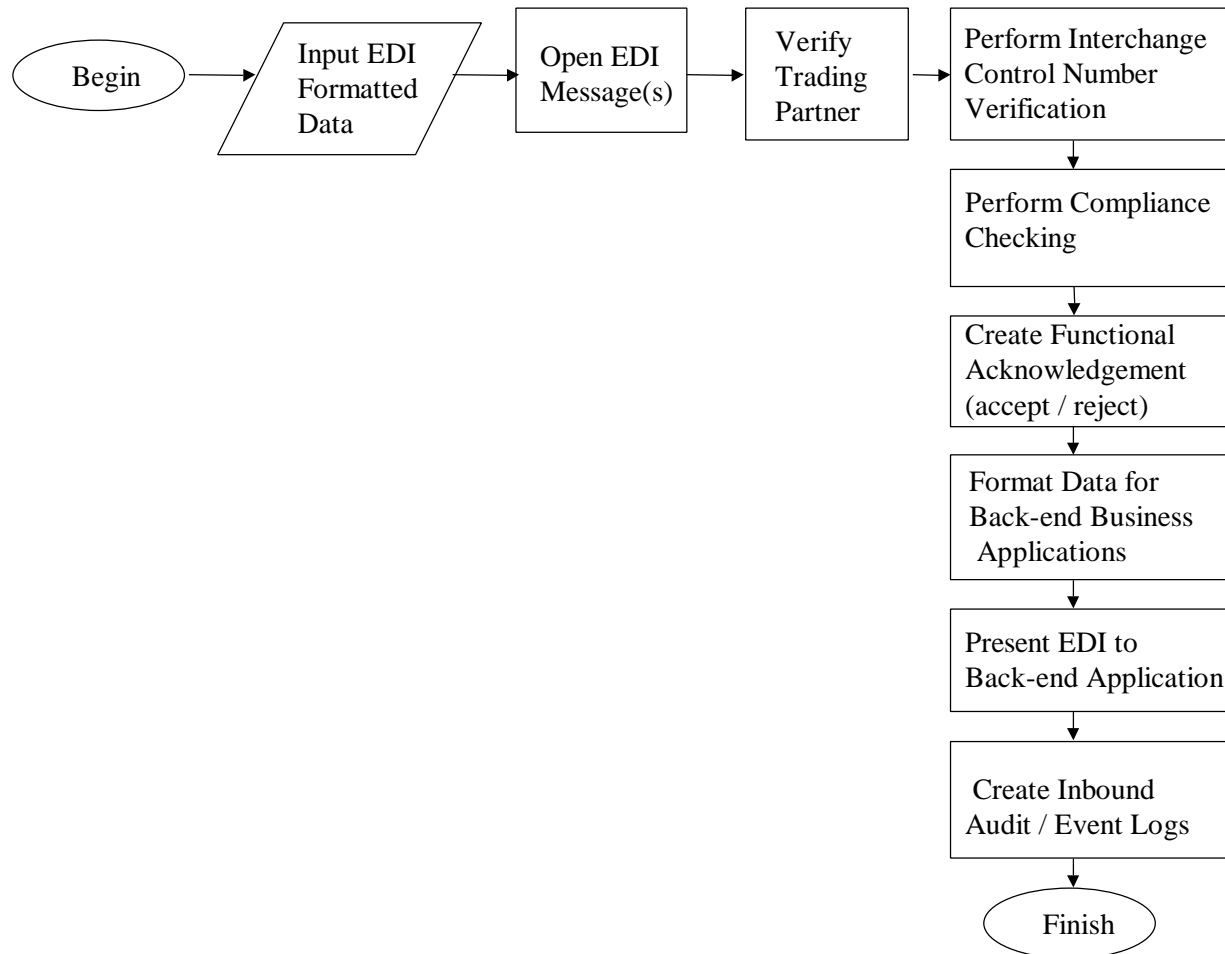


Figure 2.4-1 Transaction Interpretation: Inbound

In summary, the functional areas for this layer involve the following:

1. Process EDI message data file (i.e., unenvelope the data).
2. Verify trading partner.
3. Perform control number verification.
4. Perform EDI compliance checking:
 - Verify that mandatory fields contain data (e.g., date and invoice number).
 - Verify that the optional and conditional requirements of the data are satisfied.
 - Verify that correct data types are used (i.e., alphabetic, alphanumeric, numeric).
 - Verify data sequence by element, segment, transaction set/message, and by batch.
5. Functional Acknowledgment Creation.
6. Format and write data to internal business application.
7. Create and maintain audit logs and error logs.

Preliminary analysis of the test suite matrix reveals the following two test sets for Layer 4 of the testing model:

1. Transaction Interpretation - Data Test Set.
2. Transaction Interpretation - Software Test Set.

2.5 Layer 5: Application Interface: Inbound

The inbound application interface layer represents the interface between the Government AIS and their EDI translation/transaction system. Transactions are entered via the AIS and translated to a UDF readable by the EDI translator as illustrated in Figure 2.5-1.

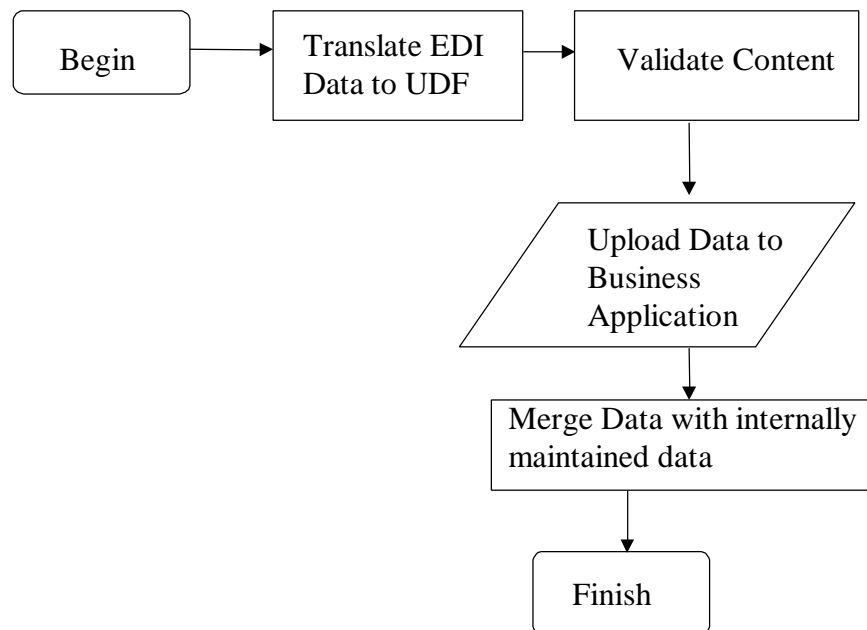


Figure 2.5-1 Application Interface: Inbound

In summary, the functional areas for this layer involve the following:

1. Supports internal business function.
2. Perform data translation (export) from EDI to UDF format.
3. Validates information content.
4. Updates business application database.
5. Merges EDI data with internally maintained data.

Preliminary analysis of the test suite matrix reveals the following three test sets for Layer 5 of the testing model:

1. Application Interface: Inbound - Application Interface Test Set.
2. Application Interface: Inbound - Data Test Set.
3. Application Interface: Inbound - Software Test Set.

3.0 TEST SCHEDULE

3.1 Test Planning, Scheduling, and Resources

It is important for successful testing programs to be well planned before they are applied. Effective testing requires planning, strategy, and discipline. A preliminary plan of actions and milestones for testing the ORDERS prototype using the above aforementioned approach is outlined below.

Table 3.1-1 Testing Schedule

Milestones	Dates
Registration with CCR.	2/1/99 – 3/1/99
Develop new test architecture and scenario.	2/19/99
Identify system requirements for NT Server based on Oracle 8i and Mercator/TPPC.	2/19/99 – 2/22/99
Install and configure NT Server Dedicated Test Platform.	3/16/99 – 4/2/99
Follow up and Collaborate with JECPO.	ongoing
Complete CAQ and submit registration.	3/19/99 – 3/21/99
Acquire Mercator; Install and configure application.	3/19/99 – 4/23/99
Mercator training.	3/26/99 – 5/15/99
Build capability in-house prior to JITC testing.	3/27/99 – 4/16/99
Conduct interoperability testing with ECI.	4/16/99 – 4/30/99
Begin development of testing approach/implementation.	4/16/99
Conduct Task 3 tests, record results, analyze results.	5/1/99 – 6/30/99
Document results and findings.	7/1/99 – 7/31/99
Develop outreach approach and package.	8/1/99 – 8/30/99
Finalize deliverables.	9/1/99 – 11/30/99

3.2 Government Activities

Government involvement includes coordination with the Joint Electronic Commerce Program Office (JECPO) and Defense Information Systems Agency (DISA) Center for Standards to assist in the development of the final test plan, and cooperation with the EDI operations team within DISA to accommodate particular ECI related testing requirements. Additionally, all relevant details pertaining to the local EC/EDI processing and communications configuration must be considered in developing the testing procedures.

3.3 Test Report

The purpose of the test report is to document test information necessary to perform testing on the UN/EDIFACT ORDERS message as described within Section 5.0. This report will be divided into four sections. Section I will contain an introduction to the UN/EDIFACT ORDERS message testing for Task 3. Section II will contain test case procedures that were performed for the

outlined testing. Section III will contain a data mapping guide which will provide the functional group segment information targeted for this testing. Section IV will contain the test results and conclusions.

3.4 Outreach

A strategy document will be developed which will inform industry and companies of the status of efforts to migrate purchasing functionality from X12 to EDIFACT. An information package will be developed to support the outreach strategy.

4.0 TEST METHODOLOGY

The objective of defining and assessing requirements is central to the concept of testing. If requirements are not consistent, it is impossible too optimally and accurately design, and more importantly for this task, to test. Therefore, this section provides an overview of the testing methodology proposed for testing the prototype implementation of the ORDERS message. It addresses the definition of testing requirements, a standard “verdict” criteria, and a standard methodology for reporting the results of the testing.

4.1 Testing Strategy

The testing scenario will involve introducing the new prototype approach (UN/EDIFACT ORDERS message) to the electronic procurement process within selected existing DoD business environments, and measuring the successfulness (validation) of this pilot approach. In order to accurately measure the degree of success, it is important to utilize an effective strategy for the testing process. The testing methodology employed for this task will be based largely on the requirements (black box testing) for the prototype test environment. This testing approach is often referred to as “dynamic testing” because it requires execution of the application program. Many of the basic functions will be tested utilizing this black box technique. Some additional syntactical testing (glass box or white box testing) will also be required, for example, when testing EDI formatted data files for compliance with the UN/EDIFACT standard. This testing approach is often referred to as “static testing” because it does not require execution of the application program. An additional test strategy, negative testing, involves attempting to prove that a requirement condition has not been satisfied or has been violated. This approach may be utilized in certain cases, for example, to ensure that only the valid range of data values are accepted as input. Utilizing this combination of strategies as a hybrid approach to testing will cover not only *what* the prototype system does from a functional standpoint but also *how* the system performs.

4.2 Assumptions and Constraints

The intent of Task 3, as defined in the statement of work, is to test the UN/EDIFACT ORDERS message to validate the adequacy of the message against actual requirements. In order to perform this test several assumptions have been made in regards to the testing environment and have been included within this report for reference. The major assumptions made in designating tests for Task 3 include the following:

- ManTech will represent the testing agents for Task 3 testing.
 - ManTech will act as the Government Trading Partner (GTP) for point of origin of the UN/EDIFACT ORDERS message to be sent.
 - ManTech will act as the Industry Trading Partner (ITP) for point of destination of the UN/EDIFACT ORDERS message to be received.
- At a minimum, the Task 3 test scenarios will cover the FEDORDER Implementation Convention.

- There may or may not be translation of the EDIFACT message within the ECI. An EDIFACT capable translator will therefore be required at point of message origin and point of message destination.
- A VAN will not be used during Task 3 testing. ManTech will apply for ECI Provider access through the ECIP.
- The Internet (TCP/IP and SMTP) will be used for communications with the ECI.
- The World Wide Web (WWW) will be used to submit, send, and receive EDI messages whenever applicable.
- New technologies such as XML will be incorporated into the test scenario whenever applicable.

Since DISA has not formally approved FEDORDER D.97A as an implementation convention it is currently not implemented within DoD certified VANS. Therefore, testing cannot rely upon translation to be performed within the VAN infrastructure unless DISA configures VAN support for Task 3 testing.

Task 3 will be performed with ManTech accessing the ECI directly via File FTP or SMTP. This will be accomplished by ManTech submitting a Client Application Questionnaire (CAQ) to the Electronic Commerce Interoperability Process (ECIP) requesting access as an ECI Provider. ManTech will operate as an ECI Provider on its own behalf, and does not intend to act as a Provider for other commercial Trading Partners (TPs). Translation will be performed locally either via Mercator and Trading Partner PC or using the ECPN's translation capabilities.

ManTech will bypass the use of Industry Trading Partners and simulate their use in-house as depicted in Figure 4.2-1. Multiple "test" trading partner accounts will be simulated using the ECI. ManTech will also simulate the Government if possible. If a reasonable simulation of Government access cannot be performed in-house, then Government agencies may be used as testing agents. If no Government agencies are available for use as testing agents, ManTech will simulate the Government segment of the test and document potential problems within the final test report deliverable.

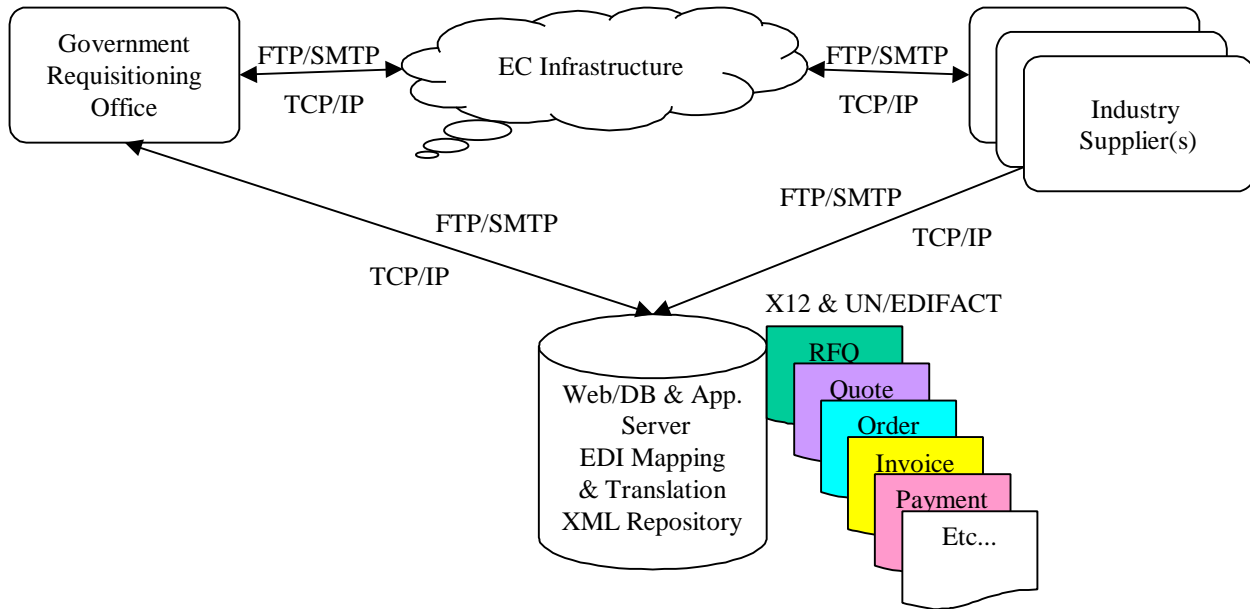


Figure 4.2-1 ManTech Testing Agent DataFlow

Since the intent of Task 3 is to validate the adequacy of the UN/EDIFACT ORDERS message, it has been assumed that generic VAN functions (i.e., send/receive transactions, data logging, response time, etc.) have been adequately tested in the certification process. Furthermore, it has been assumed that translation software packages have been adequately tested prior to being released for sale. These areas are not associated with the testing of the UN/EDIFACT ORDERS message and therefore do not require additional testing within the scope of this task. However, since DoD certified VANS have not yet been certified for UN/EDIFACT transactions, syntax and semantics associated with the UN/EDIFACT ORDERS message is considered applicable.

In particular, certain performance features outlined in Table 2.0-1, Architectural Framework Model Areas, have been deemed unnecessary for inclusion in testing under this task due to their fundamental and system specific nature. These features include:

- Network Communications
 - Transmission/Reception Performance Time
 - Reliability
 - Response Time
 - Data Retention
- Translation
 - Performance Time
 - Bounds Testing
 - Error Handling
 - Authentication
 - COTS Translation Syntax and Semantics Handling

While relevant areas of concern, these features are dependent on the VAN service selected, the translation software chosen, and the individual habits of a specific trading partner. These features lend only to the ability of the system to handle workload as deemed appropriate and the content of the applications used in the EDI transaction. Issues resulting from these areas should be handled within VAN certification, translation software package verification, and by the individual trading partners as the demands for electronic commerce grow over time. These features do not pertain to the adequacy of the EDIFACT ORDERS message in relation to the ANSI X12 standards that are currently in place. Therefore, these performance features are assumed to be out of scope with respect to the validation of the UN/EDIFACT ORDERS message and associated processing requirements.

4.3 Risk Assessment

Using EC/EDI, documents are transmitted, received, and processed automatically with minimal human involvement. Risks arising from an error in a message, or a failure in communication, are not uncommon in an electronic environment. Because of the potential for extensive legal exposure as a result of risks involving EDI systems communication, operation, and administration, prudence necessitates that a risk assessment be performed. This assessment reveals potentially jeopardizing situations that might occur during the electronic purchase ordering process. As a result of the risk assessment, the overall coverage of the testing process will be broadened to attempt to reduce the risk to an acceptable level or eliminate it entirely. The overall risk assessment will progress in the following five steps:

1. Identify Risks.
2. Assess the Potential Negative Impact of the Risk.
3. Establish Control Objectives.
4. Prioritize and Categorize Risks and Control Objectives by Functional Area.
5. Incorporate Risks and Control Objectives in the Testing Process.

4.3.1 Risk Identification and Impact

Risks have been identified from both an analysis of the electronic procurement process and the utilization of common risk checklists for automated business applications. Preliminary risks identified thus far are categorized in the following three areas and include:

1. Communications/Network
2. Operational
3. Administrative

4.3.1.1 Communications/Network

Communications/Network risks involve potential problem areas that could occur during the transmission or reception of EC/EDI data. Risks of this type may be categorized into the following four areas:

1. Communication system failures.
2. Performance problems.
3. EDI message transmission problems.
4. Unauthorized line accesses.

Communication system failures might include the service interruptions due to problems with the communication lines, VAN, Gateway, ECPN, Government Contracting Agency, or the Industry Trading Partner. The impact of a communication system failure risk is highly negative. Interruption of service due to communication system failures can potentially result in lost business due to incomplete fulfillment of orders. Also, potential loss of revenue can occur due to the inability to obtain payment for goods or services shipped, or loss of business due to breach of agreement between service provider and trading partner or between trading partners can occur.

The second type of communications/network risk identified, performance problems, addresses delays in transmission and or reception of data among trading partners and or within the ECI architecture. Again the impact of the inability to deliver critical time-sensitive EDI transactions could have a highly negative impact, which could result in loss of revenue and or breach of agreement between service provider and trading partner or between trading partners. In the case of relatively small delays, the risk will typically only result in a minor inconvenience.

The third type of communications/network risk identified, transmission problems, specifically addresses incomplete, lost, missing, duplicative, and or garbled messages being transmitted and or received among trading partners, as well as the possibility of EDI messages being sent and or received from the wrong trading partner. The impact of receiving incomplete, erroneous, or errant EDI messages could result in incorrect orders (types, quantities, destinations, etc.) being shipped, orders being shipped, or payment for goods or services shipped sent to wrong trading partners, etc. Loss of revenue or assets for suppliers, deprivation of goods/services for buyers, and or breach of agreement between service provider and trading partner or between trading partners could result in this case.

An additional area of risk, unauthorized line access, addresses unauthorized access to the EC/EDI communication via inside lines, via outside lines, or via VAN lines. Valuable information could be potentially extracted by tapping lines carrying EDI transmissions. Risks resulting from unauthorized line access could potentially be devastating and result in loss of business and or assets.

4.3.1.2 Operational

Operational risks involve potential problem areas that could occur during the normal day-to-day operation of EC/EDI systems. Risks of this type may be categorized into two basic categories as follows:

1. Unintentional
2. Intentional

The first type of operational risks identified, unintentional errors, addresses areas of risk induced by invalid information introduced in the EC/EDI. Unintentionally induced errors include system errors such as translation errors, time-date errors (e.g., year 2000), and invalid operator inputs/outputs.

The second type of operational risks identified, intentional errors, addresses areas of risk maliciously induced by a human perpetrator. Intentional errors typically include either a falsification of information and or a violation of security. Intentional errors may include entering false information, or altering existing information without authorization. Security violations include falsely assuming the identity of a different trading partner, and or denial of receipt.

The impact of operational risks can be very negative. Erroneous information (intentional or unintentional) can potentially result in lost business due to incomplete fulfillment of orders. Also, potential loss of revenue can occur due to the inability to obtain payment for goods or services shipped, or breach of agreement between service provider and trading partner or between trading partners, and having EDI messages sent to the wrong trading partner, or received from the wrong trading partner.

4.3.1.3 Administrative

Administrative risks are potential problem areas that could occur during the process of overseeing the EDI process. One of the fragile characteristics of the EC/EDI process is the absence of paper. The nature of the paper document lends itself to be legally considered as acceptable as evidence. It is tangible, lasting, and revisions are typically clearly visible. The electronic document however is quite different. It takes the form of a magnetic medium whose data content can be changed at any time. Revisions (or falsifications) to the electronic document are not always as discernible. Risks of this type may be characterized as paperless and include loss of audit trail between trading partners, loss of accounting transactions, lack of data retention, and storage media mishandling. The impact of this area can result in ineffective auditability of financial information and transaction histories. In the case of trading partner disagreements, legal disputes, or tax audits, the loss of an audit trail to verify financial and or operational transactions could result in serious consequences. When considering the communication/network area, there is always a risk that something may go wrong. The question, who should carry this risk and what should the consequences be?

4.3.2 Control Objectives

Controlling risk in electronic commerce is an ever-consuming topic in today's electronic world. Companies performing EDI have typically relied on VANs as a conduit to conduct their business through. The emerging use of the Internet as an EDI path provides alternatives to VANs. With the growing use of the electronic commerce, market place issues such as data integrity, access control, confidentiality, and user identification and authentication are the forefront of concern. These issues are reflective of the risks identified in the analysis of the electronic procurement process in Subsection 4.3.1: communication system failures, performance problems, message transmission problems, unauthorized access, unintentional operational errors, administrative concerns in regards to moving to a paperless environment. While for every solution there will always be an exception; there are avenues to drive the electronic procurement process towards for a more secure working environment if the levels of risk and vulnerability outweigh the cost to the company.

Internet Firewalls can minimize issues with access control. Internet Firewalls are generally installed between an organization's network and the Internet, thus providing a central point at which security measures can be concentrated. Internet firewalls maintain a level of segregation between an organization's network and the Internet that is conducive to good security while permitting the necessary level of connectivity to specified users.

Virtual Private Networks (VPNs) are a specialized form of encrypted Internet transactions allowing a secure channel (or tunnel) to be established between two systems for the purposes of electronic data interchange. There are currently hundreds of retail operations depending upon just-in-time inventory replacement. The data that triggers the delivery from the manufacturer travels electronically from the store, currently over private lines. If public lines (i.e., the Internet) are used, the potential for intentional disruption is enormous, not to mention the current lack of protection against accidental service outages.

Within ECI, communication to and from the Government is handled through an ECI Provider. An ECI Provider is a Federal Government department, service, or agency; a commercial VAN; or other entity that transmits, receives, sorts, and provides access to EC messages and/or transactions, via the DOD ECI. If a VAN is chosen as the preferred method of connection, potential users should realize that all VAN services will vary in the security protocol implemented, accessibility to the Internet, administrative services provided, etc. Therefore, potential users should review several VAN's services for a best fit for the company. All VAN services tend to be extremely reliable, but as with any type of highly sophisticated telecommunications, there is always a chance of interruption or delay. Although it is impossible to eliminate the possibility of interrupted service for technical reasons, some VANs will provide a backup or archive retrieval service which should capture most of the EDI data that might otherwise be lost. Internet EC/EDI also deals with service interruptions, however while the ISP works to correct their problem the user may be left without service. To minimize the effect of this type of outage, the user could opt for a secondary Internet Service Provider to provide redundant network coverage and thus minimizing the blackout potential.

Distinguishing specified users, authentication, or ensuring that users and computers are who they claim to be by establishing proof of identity. This is usually accomplished based biometrics (e.g., such characteristics as a voice pattern, handwriting or a fingerprint), a personal code [e.g., a password, Personal Identification Number (PIN), or cryptographic key] or a token (e.g., a credit card or a smart card). Technology such as digital signatures can improve authentication by improving the level of confidence in the integrity of a message. Digital signatures are based on mathematical encryption algorithms an attest to the contents of a message as well as its author. Digital signatures are based on public key, or asymmetric encryption. Asymmetric cryptography uses key pairs, one key in the key pair is called the public key and the other is called the private key. Either key can be used to encrypt the message, but once encrypted only the other key in the pair can be used to decrypt it. Therefore, by encrypting the message using the receiver's public key, the sender is assured that only the receiver can decrypt it confidentially. To digitally sign a message the sender passes the message through a hashing algorithm to produce the message digest that he then encrypts with his private key. The output is called a digital signature and is attached to, and sent with, the message. In order to verify the signature the receiver also passes

the message through the same hashing algorithm to re-create the message digest, and then decrypts the sender's digital signature using the sender's public key. If the message did not originate from the sender, or if its contents were altered, then the two digests will not match.

Where it is necessary to protect the confidentiality, integrity or non-repudiation of information, cryptographic techniques should be considered for protecting certain types of data exchange including protectively marked information. The use of public key cryptography has made possible many developments in security technology. If each user can keep their private key completely private, and make their public key completely public then confidentiality, integrity, authentication and non-repudiation are possible in many different applications, removing many of the threats posed by the use of open networks. However, making a public key public introduces many new problems of its own. The problem is that all of the mechanisms commonly used for advertising public keys are insecure themselves. One solution to this problem is certification, where rather than distributing a public key, a public certificate is advertised. This is a package combining a user's identity, the user's public key, validity information and a digital signature appended by a third party [a Certification Authority (CA)] confirming their belief in the binding between the identity and the public key for the interval of the validity. If a user requiring someone else's public key to know something about the CA that signed the certificate, then they can determine if the certificate has maliciously or accidentally been modified.

Incorporating new mediums into business processes always imposes upon individual's comfort zones. As EDI becomes a working known, today's risk will be diminished due to an increased level of understanding of the process.

4.4 Test Requirements

One of the first steps in the test planning process is defining the requirements that are to be verified. Requirements were drawn from current and existing electronic commerce documentation such as the ECI Handbook, DoD EDI Standards and Conventions Federal Implementation Guidelines, Federal Government Implementation Guidelines, UN/ECE Recommendations, Federal Acquisition Regulations (FAR), and FIPS. The requirements listed in Subsections 4.4.1 and 4.4.2 of this document represent only draft requirements.

In order to facilitate the requirements identification and definition process, the following preliminary requirement categories have been established:

1. Basic Functions
2. Data Format and Content

A brief explanation of each requirement area has been provided in Subsections 4.4.1 and 4.4.2. A consistent taxonomy for cataloging the requirements was also used and is defined as follows:

1. Requirement origin.
2. Terms or conditions of the requirement, including preconditions if applicable.
3. Test type (static, dynamic, etc.).

4. Test method, if applicable.

The requirement origin will reference the source of the requirement. Terms and conditions of requirements will be expressed in complete, consistent, unambiguous, and testable terms. For the case of situational requirements (i.e., latent requirements that need to be satisfied for certain situations) all relevant preconditions will be identified and defined. The test type field denotes whether or not testing the requirement requires the execution of the software application, in which case it is referred to as a dynamic requirement. Static requirements do not require the execution of software applications. The last field, test method, will allow for an optional description of how and what is needed to prove, or disprove if applicable, that the conditions of the requirement have been satisfied. It should be noted that as particular requirements and details of the test environment are defined, they be incorporated into the test plan.

4.4.1 Basic Functions

Basic functions, at a very high level, refers to the ability to send and receive purchase orders using the ORDERS message, as well as any additional transactions that are required. This category also includes requirements pertaining to policy issues relating to Defense Information Infrastructure (DII) and ECI policy.

Policy issues that must be considered for this task include DII and ECI policy. For example when considering ECI, it is required that all communication to and from the Government be handled through a Government-certified ECI Provider. The components of the DII that are of primary interest for the purposes of this report are the elements of EC/EDI and all those that fall under the main area of communications and computer infrastructure. For a detailed discussion of this subject, refer to the CALS Integrated Data Environment Program Telecommunications Considerations Report, prepared by Don Reynolds, October 23, 1996. Requirements for this area attempt to answer the question “Does the prototype system conform with all the relevant DII policies, strategies, and initiatives?” The FAR is another potential source of regulatory requirements pertaining to the business process (purchase order) that may need to be tested. Another potential source of policy requirements is the National Archives and Records Administration (NARA). NARA is developing standards for management of Federal records created or received on electronic mail.

The following list summarizes the high level requirements that have been identified for testing pertaining to the Basic Functions category:

- 4.4.1.1 Provide the capability to send and receive purchase orders using the ORDERS message, as well as any additional transactions that are required.
- 4.4.1.2 Support EDI transmissions between prototype test partners and their DoD trading partners, as well as any other civilian agencies.
- 4.4.1.3 All communication to and from the Government will be handled through an ECI Provider.
 - a) ECI Providers may exchange transactions via the ECI using FTP or SMTP. No dialup modems will be supported.

- 1) FTP over TCP/IP. FTP can be used to send or receive ECI transactions. When using FTP to exchange ECI transactions the binary (image) transfer type must be used to allow the transmittal of non-printable ASCII characters.
- 2) Multiple interchanges may be sent in one file.
- 3) When using SMTP to exchange EDI transactions, the Multipurpose Internet Mail Extensions (MIME) should be used.
- b) The ECI Provider is responsible for the integrity of their data, and communications of EDI transactions transmitted via the ECI by the Provider.
- 4.4.1.4 Verify that the ANSI X12 and or UN/EDIFACT transactions received are intact. Transactions are deemed received only after they are successfully translated.
 - a) For all public Government transactions, the ECI Provider must reject and not forward transaction sets with syntax error(s). If a syntax error is detected in any transaction set, the transaction set shall be rejected and not forwarded. A (EDIFACT equivalent to) 997 shall be generated to reject the transaction set.
- 4.4.1.5 The prototype system will conform to all relevant DII policies, strategies, and initiatives.

Table 4.4.1-1 Basic Requirements Test Table

D=Dynamic and S=Static

Rqmt #	Terms & Conditions	Test Type D, S	Rqmt Origin	Test Conditions	Test Method
4.4.1.1	Provide the capability to send and receive POs and any additional transactions that are required.	D	Streamlining Procurement Though EC		POs are sent from simulated seller to buyer and message arrives intact and syntactically as sent.
4.4.1.2	Support EDI transmissions between test partners and DoD trading partners.	D	DoD Standards and Conventions		POs are received intact by each trading partner via VAN and internet transmissions.
4.4.1.3	All communication to and from the Government will be handled through an ECI Provider.	S	CAQ Guidelines		
4.4.1.3a	ECI Providers may exchange transactions via the ECI using FTP or SMTP. No dialup modems will be supported.	S	CAQ Guidelines		

4.4.1.3a.1	FTP can be used to send or receive ECI transactions. When using FTP to exchange ECI transactions the binary (image) transfer type must be used to allow the transmittal of non-printable ASCII characters.	S	CAQ Guidelines		
4.4.1.3a.2	Multiple interchanges may be sent in one file.	D	CAQ Guidelines		
4.4.1.3a.3	When using SMTP to exchange EDI transactions, the Multipurpose Internet Mail Extensions (MIME) should be used.	S	CAQ Guidelines		
4.4.1.3b	The ECI Provider is responsible for the integrity of their data, and communications of EDI transactions transmitted via the ECI by the Provider.	S	CAQ Guidelines		
4.4.1.4	Verify that transactions received are intact.	D	DoD Standards and Conventions		Messages retain all content as sent by seller.
4.4.1.4a	ECI Provider must reject and not forward transactions with syntax error(s). A 997 (or EDIFACT equivalent) shall be generated to reject the transaction set.	D	Streamlining Procurement Though EC		An acknowledgment is received during transmission to reject the transaction set when a syntactically error is present within the transaction set.
4.4.1.5	Prototype system will conform to all relevant DII policies, strategies, and initiatives.	S			

4.4.2 Data Format and Content

The Data Format and Content category includes requirements pertaining to the capability to convert data from standard EDI formats including ANSI X12, UN/EDIFACT, as well as the capability to automatically convert the data in User Defined File formats to and from corresponding standard EDI messages. Sources of requirements for the data structure and content include the UN/EDIFACT standards, DoD implementation conventions, Basic Ordering Agreement, and if applicable, trading partner agreements. The UN/EDIFACT rules and standards provide numerous requirements relating to the data format (structure and syntax), syntax rules, and semantics of EDI data and relationships among constituent data elements. DoD implementation conventions and the Basic Ordering Agreement relating to this prototype message

and selected purchase order could contain additional requirements pertaining to which data elements are mandatory and which are conditional as well as the format of those data elements. Furthermore, trading partner agreements, as well as implementation conventions, may contain requirements pertaining to limitations on data elements such as restricting dollar amounts or quantities for certain data elements.

The high level requirements belonging to the Data Format and Content category include the following:

- 4.4.2.1 Comply with the data format and semantics specified in the UN/EDIFACT standards for the ORDERS (FEDORDER D.97A) message.
 - a. Standard implementation conventions and mapping procedures will be used to promote adherence to standard database development rules and the use of common data dictionaries through the Government.
 - 1. Trading Partners must have, as a minimum, an automated procurement system that produces transactions that can be mapped to standard implementation conventions.
 - 2. Provide the capability to convert data from standard EDI formats including ANSI X12 and UN/EDIFACT.
 - 3. Provide the capability to automatically convert data in UDF formats to and from standard EDI messages.
- 4.4.2.2 Comply with any restrictions or limitations that are imposed by the trading partner agreement and BOA.
- 4.4.2.3 Translating ECI Providers conducting EDI business with the Government will comply with all applicable ICs. ECI Providers will have the capability to receive and send transaction sets in accordance with the Government ICs for the appropriate standards.

Table 4.4.2-1 Data Format and Contents Requirements Test Table

S=Static and D=Dynamic

Rqmt #	Terms & Conditions	Test Type D, S	Rqmt Origin	Test Conditions	Test Method
4.4.2.1	Comply with the data format and semantics specified in the UN/EDIFACT standards.	S	DoD Standards & Conventions		Data format and semantics are translated by all COTS translator without error.
4.4.2.1a	Standard implementation conventions and mapping procedures will be used to promote adherence to standard database development rules and the use of common data dictionaries through the Government.	S	Streamlining Procurement Though EC		
4.4.2.1a1	Trading Partners must have an automated procurement system that produces transactions that can be mapped to standard implementation conventions.	S	Streamlining Procurement Though EC		
4.4.2.1a2	Provide the capability to convert data from standard EDI formats including ANSI X12 and UN/EDIFACT.	S	Streamlining Procurement Though EC		Each TP has EDI applications that are UN/EDIFACT compliant.
4.4.2.1a3	Provide the capability to automatically convert data in UDF formats to and from standard EDI messages.	S			Each TP has an EDIFACT compliant translation application locally or one accessible through a VAN.
4.4.2.2	Comply with any restrictions or limitations imposed by the trading partner agreement and the BOA.	S	UNCID		Omissions from the TPA are noted by the receiver and acknowledge upon receipt. All mandatory fields of the selected PO will be represented within the transaction message.
4.4.2.3	Translating ECI Providers conducting EDI business with the Government will comply with all applicable ICs. ECI Providers will have the capability to receive and send transaction sets in accordance with the Government ICs for the appropriate standards.	D	CAQ Guidelines		

4.5 Test Results Analysis and Reporting

In order to successfully convey the outcome of the testing effort, it is important to establish a standard and consistent procedure for analyzing, interpreting, and reporting all results and

findings from the testing process. A standard format will be utilized for reporting the testing results, which will identify the testing agent, functional component area under test (as derived from the architectural framework model), test set, and the resulting test verdict. Information pertaining to each test requirement will be summarized, and included within this report.

4.5.1 Data Analysis

The evaluation of the test results is used to measure how well the prototype system performed in the test environment. In determining an optimal technique for measuring and reporting the results of the testing process, various verdict criteria must be considered. When attempting to measure the results of individual tests, simply arriving at an absolute “PASS” or “FAIL” is not sufficient because of the potential for variance among various EC/EDI system implementations. The list of four verdict criteria presented below will be used to more accurately measure the degree to which the system complies with the specified requirements.

1. Pass
2. Fail
3. Partial
4. Could Not Determine (CND)

“Pass” is to be used when the conditions of the requirement are clearly satisfied by the test. “Fail” is to be used when the conditions of the requirement are clearly not satisfied by the test. For test results that only partially satisfy the conditions of the requirement, the “Partial” verdict shall be used. For test results that are unattainable, the “CND” verdict shall be used. These four verdict criteria will be used in conjunction with test requirements specified in Section 4.4.

Data will be collected from each test as defined in Section 5 and will be analyzed by ManTech. Data comparison will include comparing the message sent to the message received. In addition, mapping will be compared against the procedures to ensure no errors were introduced into testing at this level, and any error messages received will be reviewed against the original generated message.

In the event of test case failures, when the results of software execution are not as predicted by the procedures, the results will be reviewed to determine whether the software or procedures are in error. Upon determination of the cause of the failure, the software inputs will be corrected, the procedures will be red-lined, or the issue will be noted as an insufficiency in the UN/EDIFACT ORDERS message.

Upon conclusion of test analysis, a determination will then be made as to whether the UN/EDIFACT ORDERS message was transmitted successfully. A determination will be made as to if the ORDERS message adequately filled the business needs in the purchasing process. Recommendations will be formulated based on the test data obtained and will include areas of deficiencies in regards to the UN/EDIFACT ORDERS message.

4.5.2 Test Documentation

Test procedures are used to demonstrate that the software system complies with its requirements. They define each action to be taken by the test conductors and an acceptable range of responses by the system. Test procedures will be documented within an Implementation Guide for each testing agent. A copy of the as-executed test procedures with any red-lined modifications that were made during the test, accompanied by all test data sheets or recorded data will be included within the test report.

Test logs will be used to track test progress. Test logs will show passed tests and reruns due to Fail or Partial designations of tests. Test reruns will be logged in such a way to provide an audit trail of all the tests run prior to achieving a pass designation. All abnormal suspensions of a test will be reviewed, conditions corrected when possible, and the test will be reran. Copies of the test logs will be provided so that the reader may follow the testing process and understand any test procedure revisions or test case failures that were noted during the testing process.

Test abnormalities will be documented on test incident reports. These reports will document the situations under which negative results were noted for a particular test. Incident reports will be cross-referenced with test logs. Issues noted during testing will be logged and discussed within the final results report.

5.0 FEDORDER D.97A TEST CASES

Two types of test cases will be used to test the FEDORDER D.97A message as it pertains to a simulated Government agency; one using Internet services and the second using the ECI capabilities. Several scenarios for test case coverage are provided below. Additional information from DISA and the Government trading partners are needed before definitive test cases can be developed and included within this report.

5.1 FEDORDERS D.97A Test Case Basic Information

5.1.1 Test Objective

This test shall demonstrate that the UN/EDIFACT ORDERS message within the context of BOA and simple delivery orders is adequate in functionality pertaining to X12 purchase orders for the DoD and Federal procurement organizations to perform electronic data interchange procurements using value added network service. This scenario will consist of a single purchase order compliant with FEDORDER D.97A that will be sent from the Government purchaser (ManTech) to simulated industry trading partners. The purchase order will be transmitted by the path: simulated Government trading partner to ECI to simulated industry trading partner.

5.1.2 Test Requirements

This test case will demonstrate the following requirements.

- 4.4.1.1 Provide the capability to send and receive purchase orders using the ORDERS message, as well as any additional transactions that are required.
- 4.4.1.2 Support EDI transmissions between prototype test partners and their DoD trading partners, as well as any other civilian agencies.
- 4.4.1.3 All communication to and from the Government will be handled through an ECI Provider.
 - a) ECI Providers may exchange transactions via the ECI using FTP or SMTP. No dialup modems will be supported.
 - 1) FTP over TCP/IP. FTP can be used to send or receive ECI transactions. When using FTP to exchange ECI transactions the binary (image) transfer type must be used to allow the transmittal of non-printable ASCII characters.
 - 2) Multiple interchanges may be sent in one file.
 - 3) When using SMTP to exchange EDI transactions, the Multipurpose Internet Mail Extensions (MIME) should be used.
 - b) The ECI Provider is responsible for the integrity of their data, and communications of EDI transactions transmitted via the ECI by the Provider.

- 4.4.1.4 Verify that the ANSI X12 and or UN/EDIFACT transactions received are intact. Transactions are deemed received only after they are successfully translated.
- a) For all public Government transactions, the ECI Provider must reject and not forward transaction sets with syntax error(s). If a syntax error is in any transaction set, the transaction set shall be rejected and not forwarded. A 997 (or EDIFACT equivalent) shall be generated to reject the transaction set.
- 4.4.1.6 The prototype system will conform to all relevant DII policies, strategies, and initiatives.
- 4.4.2.1 Comply with the data format and semantics specified in the UN/EDIFACT standards for the ORDERS (FEDORDER D.97A) message.
- a. Standard implementation conventions and mapping procedures will be used to promote adherence to standard database development rules and the use of common data dictionaries through the Government.
 1. Trading partners must have, as a minimum, an automated procurement system that produces transactions that can be mapped to standard implementation conventions.
 2. Provide the capability to convert data from standard EDI formats including ANSI X12 and UN/EDIFACT.
 3. Provide the capability to automatically convert data in UDF formats to and from standard EDI messages.
- 4.4.2.2 Comply with any restrictions or limitations that are imposed by the trading partner agreement and BOA.
- 4.4.2.3 Translating ECI Providers conducting EDI business with the Government will comply with all applicable ICs. ECI Providers will have the capability to receive and send transaction sets in accordance with the Government ICs for the appropriate standards.

5.1.3 Software Test Environment

This test will be performed using EDIFACT compliant mapping tools. Each testing agent will be responsible for acquiring and configuring these tools in accordance with the EDI Transaction Set Definition for ORDERS –Purchase Order (To Supplier) for EDIFACT Version FEDORDER D.97A as provided in the Implementation Guide. Each testing agent will provide to ManTech a listing of all tools and applications (i.e., E-Mail, translation software, mapping applications, etc.) including version numbers, to be used during the testing process.

5.1.4 Hardware Test Environment

This test shall be performed using an ECI Provider. Each testing agent will be responsible for acquiring access to the ECI. Each testing agent will be responsible for maintaining electronic mail service for the disposition of test inputs and results during the testing phase.

5.1.5 Installation, testing, and control

As stated in Section 4.2 of this report, Task 3 will not perform testing of VAN systems or commercial translation software packages. Commercial software will be installed in accordance with vendor instructions. Successful installation will be taken as evidence of proper operation of the product. Successful implementation of testing required by the ECIP to become a registered user will be taken as evidence of proper operation of the hardware system between the ECI and the testing agent.

An implementation guide will be provided by ManTech to testing agents prior to testing to provide the information necessary to exchange business documents, according to the FEDORDERS D.97A ORDERS message, electronically for this simulated scenario. It will focus on mapping guides and transaction set definitions needed for this testing.

To test the transaction of the FEDORDERS D.97A ORDERS message, the simulated Governmental agency will send data according to the sample scenario provided by ManTech and the testing agent will remit the results to ManTech analysts by E-Mail, fax, or USPS. ManTech will evaluate the transmitted data and work with testing agents in a timely manner to resolve any noted discrepancies. This process will continue until ManTech is satisfied that the data is being transmitted accurately.

5.1.6 Data Recording and Analysis

Data will be filed and retained by each testing agent for shipment back to ManTech analysts for review. Each testing agent will retain the following data.

- The purchase order as it is received in a flat file format.
- A hardcopy of the data received and decoded by each testing agent's COTS translation package will be maintained.
- A copy of the mapping performed by testing agents in order to configure their EDI system.
- Any receipts of error messages received by testing agents during a test scenario.

Analysis will consist of the following activities.

- Analyze each testing agent's map to ensure consistency amongst all testers.
- Comparison of the purchase order received by each testing agent against that sent. This comparison of data will prove consistency of the data and remove reliance on any one COTS translation package.
- Any error messages will be reviewed during testing and test procedures will reflect any necessary changes.

5.2 FEDORDERS D.97A Test Case Scenarios

At this time there are several considerations that must be finalized with DISA and the Government trading partners before specific test case definitions can be formalized. This section will discuss possible test case scenarios for Task 3 testing. Figure 5.2-1 depicts the potential Task 3 Architecture. Three basic scenarios are depicted: 1) ECI is used in test and translation occurs within the ECI architecture which is representative of the current Government process; 2) ECI is used, however translation occurs outside of the ECI; and 3) ECI is bypassed and translation occurs locally. These scenarios will be presented to DISA and the Government trading partner for further clarification on the intent of Task 3 testing.

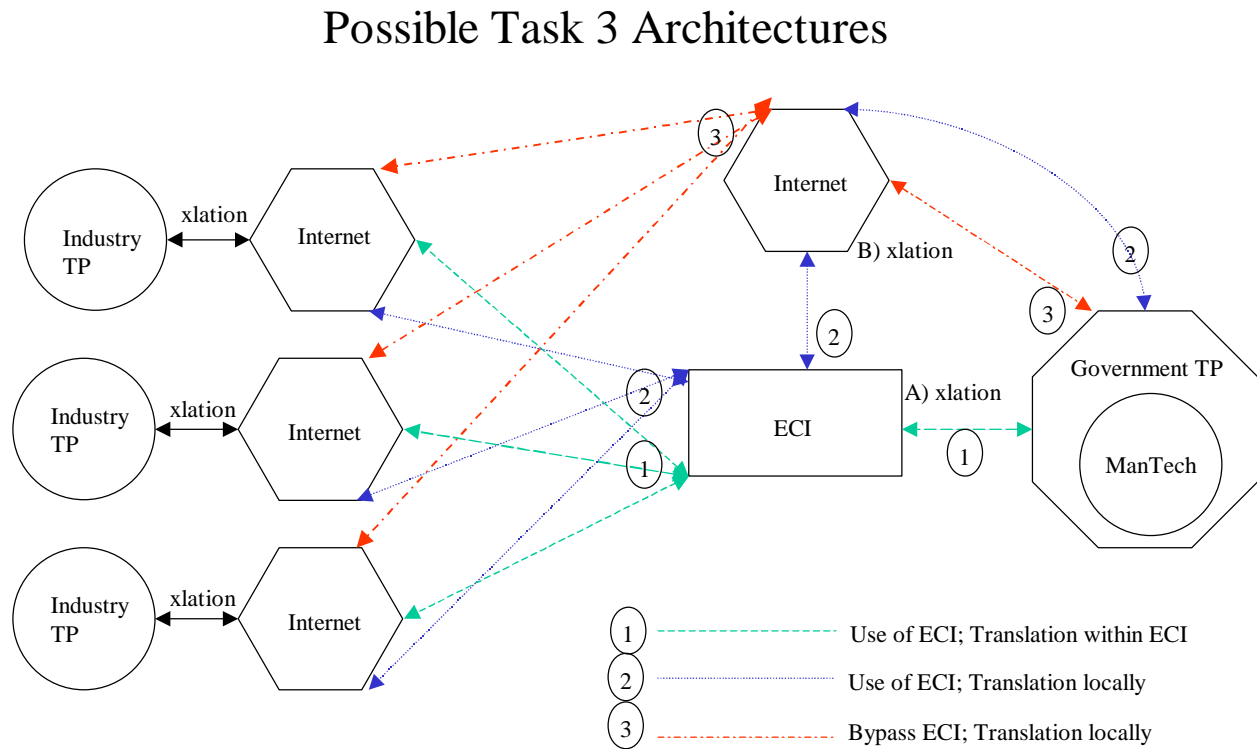


Figure 5.2-1 Task 3 Architecture

5.2.1 Scenario 1: Use ECI with translation occurring within ECI

For this scenario the ECI will be used for all transaction sets within this scenario. To provide an accurate emulation of a Government trading partner, two points should be addressed:

- 1) Translation of the transaction would occur within the ECI requiring access to a Government gateway.
- 2) A simple Government purchase order, OF 347, would be used unless DISA or a Government trading partner could provide a requisitioning form.

Translators at the Government gateway will be used for transaction set translation. This would allow Task 3 testing to mimic current Government procedures for electronic commerce.

Some issues arise, however, in the implementation of this scenario. DISA has not approved an Implementation Convention (IC) for the UN/EDIFACT ORDERS message and therefore ECI Providers and the ECI would not be available to handle the EDIFACT transaction. The Government trading partner and or DISA would need to create an arrangement with the ECIP or provide access to a Government gateway that could support EDIFACT translation and therefore provide the resources to perform this test scenario. ManTech could then work with the ECIP to create appropriate maps to support the EDIFACT testing outlined within this report. This would allow the simulated Government trading partner (ManTech) the capability to pass through the Government gateway and therefore allowing the transaction set translation to occur at the gateway. If this scenario could not be arranged translation would then occur in-house using an ECI Provider only as a conduit to access the ECI and transport the EDI message.

Due to time constraints on this testing, ManTech will simulated the industry trading partner testing. This simulated environment will dictate the level, or depth, of testing that can be performed using the UN/EDIFACT FEDORDER message. Testing will therefore range from merely receiving a purchase order request, returning acknowledgement, and following the purchase order transaction into a dummy trading partner database. This therefore limits ManTech's ability to thoroughly evaluate the UN/EDIFACT ORDERS message's capability to fulfill an industry trading partners functionality needs. It would be impossible to accurately reflect related industry needs without simulating a representative series of industry trading partner's back-end systems during the testing process.

5.2.2 Scenario 2: Use ECI with Translation Outside of ECI

Using the ECI as a pass through structure only with translation occurring at local levels for both the purchaser and supplier would not mimic a Government trading partner fully since translation does not occur at the gateway. Therefore this test would only validate the UN/EDIFACT simple purchase order message and would not utilize capabilities of the ECI structure that the Government agencies would require (i.e., gateway translation). However the scenario does allow for validation that ECI can support the capability to transfer the UN/EDIFACT ORDERS message. If translation occurred locally, an ECI Provider could be used to access the ECI. The transaction would use a simple purchase order currently used by the Government, Optional Form (OF) 347, unless another purchase order form is provided by DISA or the Government trading partner and would reflect a more global use.

Due to time constraints on this testing, ManTech will simulated the industry trading partner testing. This simulated environment will dictate the level, or depth, of testing that can be performed using the UN/EDIFACT FEDORDER message. Testing will therefore range from merely receiving a purchase order request, returning acknowledgement, and following the purchase order transaction into a dummy trading partner database. This therefore limits ManTech's ability to thoroughly evaluate the UN/EDIFACT ORDERS message's capability to fulfill an industry trading partners functionality needs. It would be impossible to accurately reflect related industry needs without simulating a representative series of industry trading partner's back-end systems during the testing process.

5.2.3 Scenario 3: Bypass ECI with Local Translation

This scenario bypasses the use of the ECI completely. Communications may be via an ECI Provider or the Internet if translation may occur locally. This scenario is in no way indicative of the Government procurement process or evaluates the ECI's capability to handle the EDIFACT transaction but does support the validation of the UN/EDIFACT ORDERS message and provides the ability to evaluate whether the message fulfills the needs of the industry trading partners involved in the test.

Due to time constraints on this testing, ManTech will simulated the industry trading partner testing. This simulated environment will dictate the level, or depth, of testing that can be performed using the UN/EDIFACT FEDORDER message. Testing will therefore range from merely receiving a purchase order request, returning acknowledgement, and following the purchase order transaction into a dummy trading partner database. This therefore limits ManTech's ability to thoroughly evaluate the UN/EDIFACT ORDERS message's capability to fulfill an industry trading partners functionality needs. It would be impossible to accurately reflect related industry needs without simulating a representative series of industry trading partner's back-end systems during the testing process.

6.0 SUMMARY AND CONCLUSIONS

This report is a draft document and will continue to be updated in the future. The U.S. Department of Defense has been working through the Pan American EDIFACT Board to augment the ORDERS message in order to satisfy DoD requirements. Because continuing changes to the ORDERS message will have an impact on this task, we must continue to be sensitive to this issue. Future versions of this report will reflect changes triggered by new releases/versions of the ORDERS message. In addition, specific details pertaining to test requirements and test procedures will be included, as they become available from industry and Government.

A five layered architectural framework model shows that there are approximately 31 functional areas and 17 product areas to be accounted for when developing the test plan. An approach for defining requirements, which considers the importance of complete, consistent, unambiguous, and testable requirements, has been established. Preliminary requirements are categorized in the following two areas (1) Basic Functions and (2) Data Format and Content. Definitions for each of the requirements have also been established. The risk assessment discusses potential risk areas and their impact. Risks are categorized as either communications/network, operational, or administrative related and consist primarily of system failures, errors, or security breaches. As additional information pertaining to requirements, risks, and testing becomes available, it will be incorporated into the test plan deliverable.

The results from these tests will be compiled into a collection of test analysis reports, which will document findings, conclusions, and recommendations resulting from the overall testing process. At the micro level, the test analysis will help reveal deficient product and/or functional areas relating to the prototype message. At the macro level, this analysis will consider the operational, organizational, and technical perspectives relating to the degree of success achieved by this prototype and in turn the following questions should be answered:

1. How well does the UN/EDIFACT ORDERS message support the requisite objectives of the organization?
2. How capable is the UN/EDIFACT ORDERS message in achieving the functionality required?
3. Is the UN/EDIFACT ORDERS message acceptable to the Government, industry, and end users?

APPENDIX A: GLOSSARY

APPENDIX A: GLOSSARY

Acceptable Level of Risk - A judicious and carefully considered assessment by the appropriate accrediting authority that the value of the Automated Information System (AIS) or network unambiguously outweighs the likelihood of potential damage to the security interests of the United States in the event information from the system is compromised, damaged, or destroyed. The severity of the potential damage must be taken into account. The assessment should take into account the value of AIS or network assets, threats, and vulnerabilities, as well as countermeasures and their ability to compensate for vulnerabilities and operational requirements.

American National Standards Institute (ANSI) - The principal standards coordination body in the United States. ANSI is a member of the International Organization for Standardization (ISO).

Archive - To store data for a given period of time for security, backup or auditing.

Automated Information System (AIS) - Computer hardware, computer software, telecommunications, information technology, personnel, and other resources that collect, record, process, store, communicate, retrieve, and display information. An AIS can include computer software only, computer hardware only, or a combination of the above.

Basic Ordering Agreement - A basic ordering agreement is a written instrument of understanding, negotiated between an agency, contracting activity, or contracting office and a contractor, that contains terms and clauses applying to future contracts (orders) between the parties during its term, a description, as specific as practicable, of supplies or services to be provided, and methods for pricing, issuing, and delivering future orders under the basic ordering agreement. A basic ordering agreement is not a contract.

Black Box Testing - A test strategy that focuses on testing “what” the system is required to do from a functional point of view.

Business Application - A computer-based system that process business information in support of a specific business function such as purchasing, accounting or logistics management, etc. Business application data is produced by such applications and transmitted to a translation program for conversion into an EDI format, and vice versa.

Communications Handler - A software program that controls computer hardware and modems and arranges for the transmission or reception of electronic data.

Compliance Checking - A checking process that is used to ensure that a transmission complies with syntax rules.

Control Characters - In communications, any transmitted characters used to control or facilitate data transmission between two or more computers. Also, characters associated with addressing,

polling, message delimiting and blocking, framing, synchronization, error checking, and other control functions.

Control Structure - The beginning and end (header and trailer) segments for entities in Electronic Data Interchange.

Data Element - The smallest, meaningful piece of information in a business transaction. A data element may condense lengthy descriptive information into a short code. Equivalent to a data field in a paper document; a series of data elements are used to build a data segment. A data element dictionary that defines the data element and, where appropriate, the code is part of ASC X12 or UN/EDIFACT standards.

Data Element Delimiter - A separating character, such as an asterisk (*), that precedes each data element within a segment.

Data Element Dictionary - The publication that lists all of the data elements used within EDI standards.

Data Segment - A data segment is a group of related data elements in a transaction set. Each segment has a unique segment identifier, a combination of two or three uppercase letters and/or digits that serves as a name for the segment and occupies the first character positions of the segment. A segment is equivalent to a data record in a database.

DoD EC and EDI Infrastructure - A subset of the Defense Information Infrastructure (DII) that is designed to support EC and EDI. It is composed of hardware, software, and people. It provides services such as translation, archiving, distribution, and result notification. It supports all DoD EC and EDI functional activities as well as other civilian agencies that may need to use it.

DoD Gateway - DoD Gateways control the timing and flow of EDI transactions on the Government side of ECI.

Dynamic Requirement - Testing of dynamic requirement types requires the execution of the software application.

Dynamic Testing - Requires execution of application to accomplish testing.

Electronic Commerce (EC) - The paperless exchange of business information (goods and services) or ideas using Electronic Data Interchange (EDI), Electronic Mail (E-Mail), electronic bulletin boards, Electronic Funds Transfer (EFT), facsimile, video conference, and other similar technologies.

Electronic Commerce Processing Node (ECPN) - A collection of hardware and software systems which provides communications connectivity between Value Added Networks (VANs) and the Government Gateways to support the exchange of EDI transactions between Government procurement agencies and private sector Trading Partners. There are currently two ECPNs, located in Columbus, Ohio and Ogden, Utah.

Electronic Data Interchange (EDI) - The computer-to-computer exchange of business transaction information in a public standard format.

Electronic Mailbox - A holding location for EDI transactions generally provided by a Value Added Network (VAN) to its customers. The customers would normally dial-up and connect to their EDI mailboxes and download and upload transactions.

FACNET - Federal Acquisition Network (FACNET) was created by Section 9001, Federal acquisition Streamlining Act of 1994, Pub. L. 103-355, October 13, 1994, 41 USC 426. FACNET is defined as: the Government wide Electronic Commerce/Electronic Data Interchange (EC/EDI) systems architecture for the acquisition of supplies and services that provides for electronic data interchange of acquisition information between the Government and the private sector, employs nationally and internationally recognized data formats, and provides universal user access. Federal Acquisition Regulations (FAR) 4.501.

FACNET is not a specific system but rather a series of capabilities. For procurements at or below the Simplified Acquisition Threshold, a contracting activity using an Interim FACNET certified system is exempted from the requirement of posting or synopsis in the Commerce Business Daily (CBD) as indicated in FAR 5.202 (a) (13) and the waiting periods required before award or issuance of the solicitation.

FTP - A file transfer protocol typically used with Transmission Control Protocol/Internet Protocol (TCP/IP).

Functional Acknowledgment - An ANSI ASC X12 Transaction Set (997) which is produced by translation software upon receiving and validating an EDI transaction set, and sent to the sender.

Glass (White) Box Testing - A test strategy that focuses on testing “how” the system accomplishes certain tasks at a very low level.

Implementation Convention - A subset of the X12 standard that represents the common practices and/or interpretations of the use of X12 standards. Conventions define how trading partners will use the standards to accommodate their mutual needs. An Implementation Convention should exist for each EDI transaction set that is to be used. Implementation Conventions deal with transaction sets at the data element level. For the Government, or any industry sector, Implementation Conventions (for doing EDI within that industry) can be highly detailed subsets of the Implementation Guidelines (for doing EDI within that industry).

Implementation Guideline - The Guideline contains instructions on the use of EDI. It provides

additional information to assist in conducting EDI. The Guideline is intended to provide assistance and should not be your sole source of information.

Inbound Transaction - A transaction coming to the receiver from the sender.

Interchange Control Number - A control number assigned to an EDI interchange that is unique to both the interchange and the trading partner for which the particular interchange.

Interim FACNET - Means a contracting office has been certified as having implemented a capability to provide widespread public notice of, issue solicitations, and receive responses to solicitations and associated requests for information through FACNET. Such capability must allow the private sector to access notices of solicitations, access and review solicitations, and respond to solicitations.

Mapping - The process of manually mapping data elements from User Defined File formats to and from corresponding standard EDI transaction sets.

Negative Testing - A test strategy that attempts to prove that a requirement condition has not been satisfied (e.g., bounds testing).

NIPRNET - N-level Internet Protocol Router Network (NIPRnet) is often referred to as the non-classified DoD intranet.

Nonrepudiation - The quality of a secure EDI system that prevents a party from falsely denying that the sent or received a specific transaction/message.

ORDERS Message - Specifies details for goods or services ordered using Electronic Data Interchange (EDI) between trading partners involved in administration, commerce and transport under conditions agreed between the seller and the buyer.

Outbound Transaction - A transaction leaving from the sender and going to the receiver.

Positive Testing - A test strategy that attempts to prove that a requirement condition has been satisfied (e.g., validation).

Public Transaction - A transaction that, rather than being sent to one trading partner, is broadcasted to a predefined group of trading partners. Alternatively, a transaction that is made available to any trading partner by being placed in a publicly accessible media, such as an electronic bulletin board, for downloading.

Requirements - The necessary conditions that apply to an object, event, or abstract assertion. Object requirements state particular properties that the object must possess. Event requirements state particular performance capabilities, or other criteria that must be satisfied. Abstract requirements pertain to conceptual notions and are not nearly as common and often subjective in nature.

Security - A generic term describing the methods adopted to protect data from loss, corruption, and/or unauthorized access and retrieval. Methods include passwords, digital signatures, identification keys, verification, encryption/decryption, and nonrepudiation of sender and receiver.

Simple Mail Transfer Protocol (SMTP) - The TCP/IP protocol for transferring electronic mail messages from one machine to another. SMTP specifies how two mail systems interact and the format of control messages they exchange to transfer mail.

Situational Requirement - Latent requirements that are invoked only whenever specific situations arise.

SMTP - Simple mail transfer protocol.

Static Testing - Does not require execution of application to accomplish testing.

Store-and-Forward - The process of storing EDI transmissions in an electronic mailbox before delivering them to recipients.

Static Requirement - Testing of static requirement types does not require the execution of the software application.

Testing - The process of exercising or evaluating a system or system component, by manual or automated methods, in order to verify that it satisfies specified requirements or identifies differences between expected and actual results.

Testing Agent - The person or entity actually performing and/or administering the testing process. Human testing agents may be classified as 1st (industry), 2nd (Government), and 3rd party (independent) testers.

Test Case - A group of related tests applicable to a particular requirement area from the specification.

Test Data - Data developed or used to test a system or system component to verify compliance with a particular requirement.

Test Report - A document describing the conduction and results of the testing carried out for a system or system component.

Test Script (Procedure) - Detailed instructions for the setup, operation, and evaluation of results for a given test.

Test Sets - A collection of Tests Cases that relate to a particular class of requirements.

Test Suite - A comprehensive group of tests covering all of the defined requirements. This can include boundary conditions, illogical test cases, and illegal test cases.

TCP/IP - Transmission communications protocol/internet protocol.

Trading Partner (External) - A non-federal Government entity with whom the Federal Government exchanges business transactions.

Trading Partner (Internal) - A Federal Government entity who exchanges business transactions with another Federal Government entity.

Trading Partner Agreement (TPA) - A written instrument of understanding negotiated agreement between EDI Trading Partners that specifies contractual matters and protocols of governing EDI transactions. These are generally used in the private sector among EDI Trading Partners. Within the Federal EDI acquisition context, Trading Partner Instructions (TPI) are issued by the Government to the vendor community and are used instead of a TPA.

Trading Partners - Entities who exchange business transactions.

Transaction - All of the business information contained in a transaction set.

Transaction Set - A semantically meaningful unit of transaction information exchanged between EDI trading partners. It can be thought of as the electronic counterpart of a paper document that represents a transaction, e.g., an invoice, a bill of lading, or a medical insurance statement.

Translation - A utility that uses the results of the mapping process to automatically convert the data in User Defined File formats to and from corresponding standard EDI transaction sets or messages.

Value-Added Network (VAN) - Generally commercial entities that transmit, receive, and store EDI transactions on behalf of their customers. VANs may also provide additional services known as Value Added Services. Also known as third party networks.

Value-Added Service (VAS) - A Value Added Service (VAS) may be a separate commercial organization (also known as an EDI service bureau) that provides EDI-related services, or a VAN that provides extra fee-based services beyond standard VAN services to its customers. Such services may range from translation to "EDI-to-FAX" services to complete EDI-integrated business systems.

Verdict Criteria - Standard method for rating the results of a test.

X.400 - The international standard developed by Consultative Committee on International Telegraph and Telephone (CCITT) for a store-and-forward message handling system in a multivendor environment.

APPENDIX B: ABBREVIATIONS AND ACRONYMS

APPENDIX B: ABBREVIATIONS AND ACRONYMS

AIS	Automated Information System
ANSI	American National Standards Institute
BOA	Basic Ordering Agreement
CA	Certification Authority
CALS	Continuous Acquisition and Life-cycle Support
CAQ	Client Application Questionnaire
CCITT	Consultative Committee on International Telegraph and Telephone
CND	Could Not Determine
COTS	Commercial Off-The Shelf
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DoD	Department of Defense
EC	Electronic Commerce
ECE	Economic Commission for Europe
ECI	Electronic Commerce Infrastructure
ECIP	Electronic Commerce Interoperability Process
ECPN	Electronic Commerce Processing Node
EDI	Electronic Data Interchange
FACNET	Federal Acquisition Network
FAR	Federal Acquisition Regulations
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GTP	Government Trading Partner
IC	Implementation Conventions
IDE	Integrated Data Environment
ISG	Industry Steering Group
ISO	International Organization for Standardization
ITP	Industry Trading Partner
JECPO	Joint Electronic Commerce Program Office
MIME	Multipurpose Internet Main Extensions
NARA	National Archives and Records Administration
NATO	North Atlantic Treaty Organization
NIPRnet	N-level Internet Protocol Router Network

OF	Optional Form
OSI	Open Systems Interconnection
PIN	Personal Identification Number
SMTP	Simple Mail Transfer Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TP	Trading Partners
UDF	User Defined Format
UN/EDIFACT	United Nations rules for Electronic Data Interchange For Administration, Commerce and Transport
VAN	Value Added Network
VAS	Value Added Service