Requirements

Communications provide trade community participants in the Automated Manifest System (AMS) the capability of transmitting data to and receiving data from the U.S. Customs computer. Customs authorizes access to the AMS for several categories of trade clients:

- Carriers
- Port Authorities
- Service Bureaus
- Rail
- Non-vessel Operating Common Carrier (NVOCC)
- Vendors

The system is voluntary and designed to use technology that is standard and readily available to both small and large businesses.

Several options are available to potential AMS participants in the U.S. Customs Communications Interface Program. Software can be developed by the client or purchased from a vendor. Another possibility is to mailbox through a Value Added Network (VAN), or, if automation is a problem, securing the servicing facilities of a port authority or service center can be done.

The preparatory steps to become an AMS participant are explained in this chapter, as well as the hardware and software requirements and testing procedures required for successfully completing the communications interface with AMS.

Respondent Checklist

A telephone call or a letter to the Manifest group begins the process of becoming an AMS participant. Call (703) 921-7501 or send a letter requesting information about the program to:

U.S. Customs Service
Client Representative Branch

Upon receipt of the inquiry, an information package is sent to the requesting organization. The package contains a Respondent Checklist, instructions on how to complete the checklist, the latest copy of this document, Master In-bond documentation, and a copy of Customs policy regarding electronic interface.

Once the Respondent Checklist has been completed and returned to Customs and the potential participant has chosen a communications technique and protocol, the participant undertakes procurement of equipment and software. A Customs representative is assigned to work with the company and serve as a technical advisor to aid in the process of becoming an AMS participant.

Figure 1*: *Dial-up Service

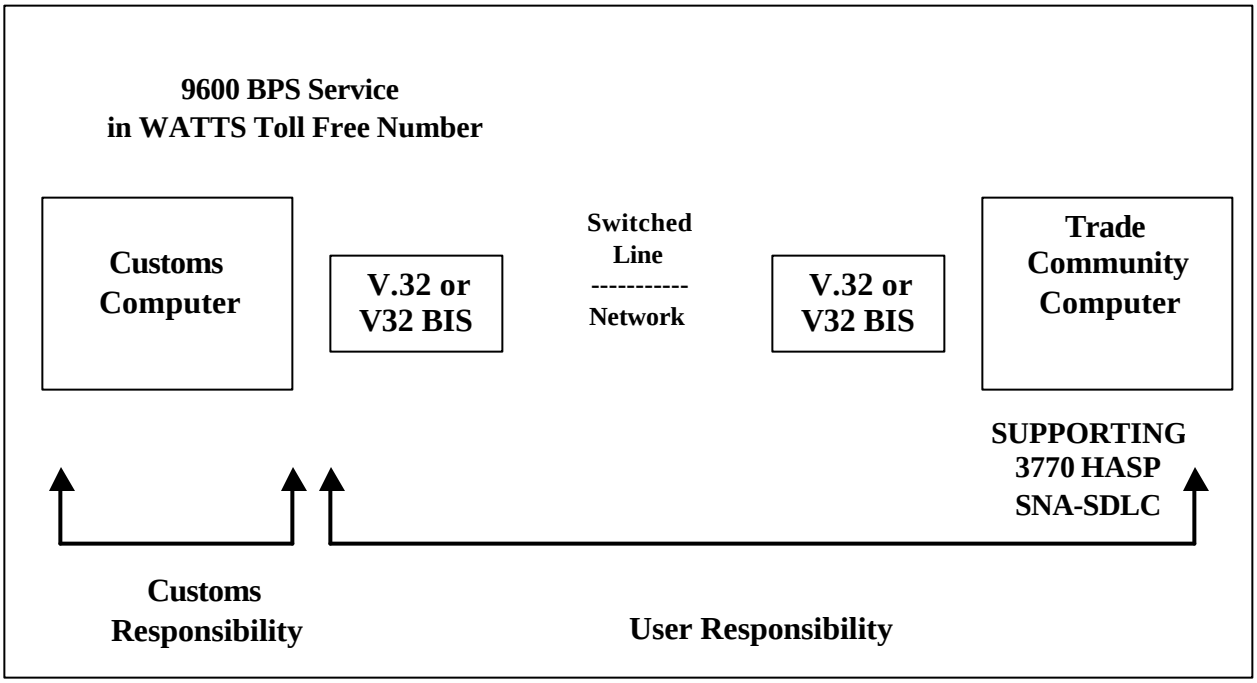
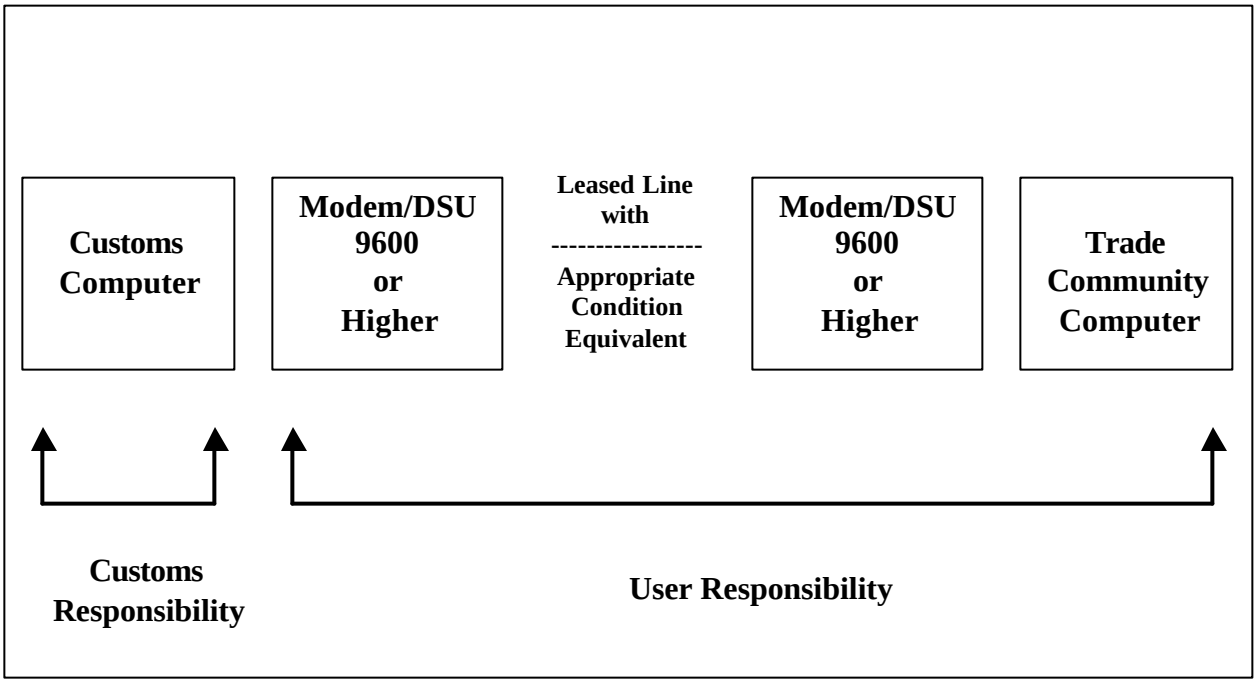


Figure 2*: *Dedicated Service



Communication Technique and Protocol

Customs provides two basic means of communications:

- Dial-up connections to the Automated Commercial System (ACS) using toll-free numbers provided by Customs (see Figure 1, previous page).
- Dedicated service through user-provided leased lines (see Figure 2, previous page).
- LU6.2 Protocol Interface
- MQ Series via Frame Relay

Potential participants decide whether to use the dial-up service or to provide leased lines, the communications speed (baud rate), and protocol. To assist in this decision, a Customs Communications Specialist is available at the U.S. Customs Service Data Center at (703) 921-6000.

Procurement of Equipment and Software

Based on communications needs, the user orders the necessary hardware (modems/DSU) and software (MQ Series). Appendices A and B of this document provide the specifications and definitions of the options currently available.

If the decision is to use the dial-up service, the toll-free number will be provided prior to the communications interface test.

Participants who choose to use the dedicated service (leased line) must undertake the following tasks:

- Purchase two (2) modems or DSUs, one of which will be placed at the U.S. Customs Service Data Center.
- Purchase two (2) link encryption unit IRE.
- Provide the following address and telephone number to the circuit and modem equipment supplier:

  Computer Center Branch
  Network Control Center
  U.S. Customs Service Data Center

  (703) 921-6375

Provide the following information to the U.S. Customs Service Data Center:

a) Organization name and address

b) Technical and management contacts' names and telephone numbers

c) The names and phone numbers of the data processing company, if the participant's system will be developed outside the company

d) The company's hardware and software procurement plans

e) Modem/DSU type

f) Speed

g) SNA 3770

h) MQ Series

i) LU 6.2

j) Circuit number

k) Name of circuit vendor

l) Date of installation

m) Name of installer

Pre-Test Requirements

When the client completes equipment procurement and software requirements and provides the information to Customs, responsibility for implementing the next phase passes to the Client Representative Branch at Customs Headquarters. The Client Representative Branch contacts the client to verify the company contact information already provided and advises the client on establishing the passwords needed to maintain a client file within the Customs database. The team also provides the client with a Customs-assigned remote number. The password requirements are:

- An applications password, created by the client, must be alphanumeric, no longer than six (6) positions.

- A communications password, must be alphanumeric, no longer than eight (8) positions. This is provided to the participant after being determined by a Communications Specialist.

Client Representative Branch personnel provide this information to a Communications Specialist at the Customs Data Center. The specialist will then contact the client to verify all communications protocol and sign-on procedures. The user's applications support program must build a file which the communications will transmit to the Customs computer.

Customs Pre-Test Responsibilities

Client Representative Branch personnel create the necessary client files in the Customs database in preparation for the communications interface test. These include files for the user, data processing site, and carrier. The Client Representative Branch also coordinates the creation of the security files with Customs System Security. Customs final pre-test responsibility is to verify the accuracy of information in the client files.

Communications Testing

A test file is placed on the output queue and made available for the new client to attempt to capture. The file contains a detailed description of the mandatory test steps, pre-pilot and pilot phases. The file also contains the Job Control Language (JCL) that the client will use to submit the test manifest. A sample manifest in the 80-column format and a sample manifest in American National Standards Institute (ANSI) format are also included in the file.

The Client Representative Branch will work to resolve communications problems encountered during this initial interface attempt between the new client and the Communications Center at the Customs Data Center.

Data Encryption Information

Since March of 1995, data encryption devices have been required in remote user sites. The Model HS-VC supports the Data Encryption Standard (DES) or ATLAS encryption for remote user sites. The remotes have no switches or controls and are simply installed between the remote terminal or PC and the modem. The HS-VC Remote Encryptor can be connected via V.35 or RS-232, and performs at data rates up to 64K bps sync or 9600 bps async.

Each remote encryptor has a front port of local configuration and four indicator lights that display its status during operation. At power-on, at least one indicator lights momentarily while the device performs self-tests. The indicator lights are:

- **CIPHER** is lit when data is being encrypted. The *cipher* indicator is green to signify that data is being safely encrypted. (In Link mode, *cipher* light is always lit.)

- **BYPASS** is lit before and during the establishment of a call in Dial mode. In Link mode, the *bypass* indicator is never lit.

- **LOCAL** is lit when the remote encryptor is connected to a dumb PC terminal via its front port. It is used in this mode for configuration purposes. The *local* indicator is red.

- **ALARM** lights if an error is detected when the remote encryptor performs its self-tests. These tests include checks of the program memory and the DES encryption hardware. The *alarm* indicator is red.

Theory of Operation

The Link Encryption System is designed to operate in *Point-to-Point* and *Multidrop* configurations. The Link Encryption System can support both small and large point-to-point systems. A remote encryptor is used at each end of the network. For Multidrop configurations, a remote encryption device will be required at each remote end with one host encryptor at the Customs Data Center.

Remote Site

Data Communication

Interface: RS-232-C or V.35
Data Rate: 14,400, 9600, 19,200 bps (V.35 64 Kbps)
Full or Half duplex

Security Standards

Data Encryption Standard certified by National Institute of Standards and Technology
Data Encryption: ANSI X3.92-1981, FIPS 46-1, ISO DIS 10126
DES Cipher Feedback Mode (8 bit): ANSI X3.106
Key Management: ANSI X9.17, ISO DIS 8732
Randomly generated key exchange for each session
Automatic check to eliminate weak session keys
Master key encrypted in non-volatile memory

Diagnostics

Automated DES S-Box test on power-up
Memory test on power-up

Security Services

Data Encryption

Initial Key Loading

The *Storage Key* must be loaded at the Customs Data Center by a designated *Storage Key Manager(s)*. The *Storage Key* will be kept in non-volatile memory and will not be lost during power loss.

Compatibility

Compatible with commonly used asynchronous and synchronous modems.

Environment

Temperature: Operating 0-50 C (32-132 F); storage 0-65 C (32-149 F)
Humidity: Operating 10-90% relative non-condensing; storage 15-95% relative non-condensing
Shock: Withstand shock associated with a 6-foot drop onto a concrete floor
Vibration: Operate after withstanding 1/2 g vibration from 2 to 200 Hz with sweep time set to 1.2 octaves per minute

Power

Input (standard): 120 VAC +/- 10%, 60 Hz, UL 478, and CSA 22.2 approved
Input (optional): 220 VAC +/- 10%, 50 Hz, GS, IEC 380/433/950, TUV Certified
Output: 9VDC, 1A

Static Electricity

Operates without malfunction withstanding up to 7 KV voltage discharge at any externally grounded part of unit

Mechanical

15x19x4 cm
6.1x7.6x1.5 inches

Ordering Information

Information Resource Engineering Inc. (IRE)
8029 Corporate Drive
Baltimore, MD 21236
Phone (410) 931-7500
Fax (410) 931-7524

Secure Computer Link System Configurations

Qty	Model No.	Description
V.35		
1	HS-VC-v.35	Remote Link Encryptor w/cable
1	MHS-VC-v.35	Host Link Encryptor w/cable, shipping and handling
RS-232		
1	HS-VC-rs232	Remote Link Encryptor w/cable
1	MHS-VC-rs232	Host Link Encryptor w/cable, shipping and handling

The IRE Link Encryption System is designed to provide encryption protection for communications over dedicated circuits. Data is encrypted at the sending location using the Data Encryption Standard (DES) and traverses the network in encrypted form until it is decrypted at the receiving location.

Delivery: Maximum 30 days ARO
Terms: Net 30 days

User Notes: