FED-STD-1028
April 04, 1985

FEDERAL STANDARD

TELECOMMUNICATIONS: INTEROPERABILITY AND SECURITY REQUIREMENTS FOR USE OF THE DATA ENCRYPTION STANDARD WITH CCITT GROUP 3 FACSIMILE EQUIPMENT

This standard is issued by the General Services Administration pursuant to the Federal Property and Administrative Services Act of 1949, as amended.

1.Scope

1.1. Description. This standard specifies interoperability and security related requirements for the use of encryption with CCITT i.e., International Telegraph and Telephone Consultative Committee) Group 3-type facsimile equipment. The algorithm used for encryption is the Data Encryption Standard (DES), described in Federal Information Processing Standards Publication 46. Requirements contained in section 3 below relate to the interoperation of DES Cryptographic Equipment, or their operation with associated CCITT Group 3 facsimile equipment. Additional security requirements, not directly relating to interoperability, are contained in Federal Standard 1027.

1.2 Objectives
1.2.1 Interoperability. To facilitate the interoperation of Government facsimile equipment that requires cryptographic protection using the Data Encryption Standard (DES) algorithm.

1.2.2 Security. To prevent the disclosure of facsimile documents.

1.3Application. This standard applies to all DES cryptographic components, equipment, systems, and services procured or leased by Federal departments and agencies for the encryption, using the Data Encryption Standard (DES) algorithm, of documents transmitted by CCITT Group 3-type facsimile equipment. Guidance to facilitate the application of this standard, with respect to degradation of security by improper implementation or use, will be provided for in a revision to Federal Information Resources Management Regulation 201-7.

1.4 Definitions. Until Federal Standard 1037 is revised to ind ude encryption terms, def initions of encryption-related terms may be found in the National Communications Security (Glossary.

2. Referenced Documents

a. Federal Information Processing Standards Publication 46: Data Encryption Standard. (Copies of this standard are available from the National Technical Information Service, U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161).
b. Federal Information Processing Standards Publication 81: DES Modes of Operation. (Copies of this standard are available from the National Technical Information Service, U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161).

c. Federal Standard 1026: Telecommunications: InteroperabAity and Security Requirements for Use of the Data Encryption Standard in the Physical Layer of Data Communications. (Copies of this standard are available from the General Services Administration Specification Unit (WFSIS), Room 6039, 7th and D Streets S.W., Washington, D.C. 20407).

d. Federal Standard 1027: Telecommunications: General Security Requirements for Equipment Using the Data Encryption Standard. (Copies of this standard are available from the General Services Administration Specification Unit (WFSIS), Room 6039, 7th and D Streets S.W., Washington, D.C. 20407).

e. Federal Standard 1062: Telecommunications: Group 3 Facsimile Apparatus for Document Transmission. (Copies of this standard are available from the General Services Administration Specification Unit (WFSIS), Room 6039, 7th and D Streets S.W., Washington, D.C. 20407).

f. Federal Standard 1063: Telecommunications: Procedures for Document Facsimile Transmission. (Copies of this standard are available from the General Services Administration Specification Unit (WFSIS), Room 6039, 7th and D Streets S.W., Washington, D.C. 20407).

g. National Communications Security Glossary (Controlled Distribution). Copies of this glossary may be requested from the National Communications Security Committee (NCSC) Secretariat, Room C-2A40, Operations Building 3, National Security Agency, Fort George G. Meade, MD 20755.

3. Requirements

3.1Overview. CCITT (i.e. International Telegraph and Telephone Consultative Committee) Group 3 digital facsimile, transmitted at 2.4, 4.8, 7.2, or 9.6 kbits/s, is encrypted using the Data Encryption Standard (DES) algorithm in the same manner as is described for encrypting synchronous data in Federal Standard 1 026. Only Group 3 facsimile documents and optional 2.4 kbit/s binary-coded signals are encrypted. Group 3 facsimile is described in Federal Standard 1062. Binary-coded signals are described in Federal Standard 1063.

3.2 Mode of Operation. The 1-bit Cipher Feedback mode of operation shall be used. (Ref. Federal Information Processing Standards Publication 81).

3.3 Transmission. Upon Clear to Send indication (e.g., CCITT Interchange Circuit 106, Ready for Sending, ON) from a primary (i.e., CCITT V.27 ter or V.29) modem, the modem input (e.g., CCITT Interchange Circuit 103, Transmitted Data) is typically in a MARK (ail ONES) state. A 48-bit Initializing Vector (IV) is sent at this point in time, preceded by a single ZERO bit (SPACE) to delimit the IV. The first bit transferred of the 48-bit IV is placed in bit position 17 of the DES device input block (Ref. Federal Information Processing Standards Publication 81). After transmission of the IV, all bits passing through the primary modem are first encrypted. Encryption continues until Clear to Send indication is turned off.

3.4 Reception. Upon Receiver Ready indication (e.g., CCITT Interchange Circuit 1 09, Data Channel Received Line Signal Detector,

ON) from a primary (i.e., CCITT V.27 ter or V.29) modem, the modem output (e.g., CCITT Interchange Circuit 104, Received Data) is typically in a MARK (all ONES) state. The 48 bits received immediately following the first ZERO bit (SPACE) are considered to be the Initializing Vector. All following bits received are decrypted. Decryption continues until Receiver Ready indication is turned off.

3.5 Encryption Bypass. Except when DES Cryptographic Equipment is in the bypass mode (reference Federal Standard 1027), it shall not be possible to transmit or receive unencrypted facsimile documents or portions thereof (including Group 1 and 2 documents).

3.6 DES Key Variable Loading. The capability shall exist to operate (i.e., encrypt and decrypt facsimile documents) with DES 5 key variables loaded using one of the two methods described in Federal Standard 1027.

4. Effective Date. The use of this standard by U.S. government departments and agencies is mandatory effective 180 days following the date of this standard.

5. Changes. When a Government department or agency considers that this standard does not provide for its essential needs, a statement citing specific requirements shall be sent in duplicate to the General Services Administration (K), Washington, DC, 20405, in accordance with the provisions of the Federal Information Resources Management Regulation 201-8.101-3. The General Services Administration will determine the appropriate action to be taken and will notify the agency.

PREPARING ACTIVITY:

National Communications System
Office of Technology and Standards
Washington, DC 20305-2010

MILITARY INTERESTS:

Military Coordinating A Review Activities NSA-NS Army-AD,CR NavyAS,OM
Custodians Air Force-90 ArmySCDCA-DC
Navy-EC JTC3A-TT Air Force02 DLA-DH

User Activities Navy-SH,MC

This document is available from the General Services Administration (GSA), acting as agent for the Superintendent of Documents. A copy for bidding and contracting purposes is available from GSA Business Centers. Copies are for sale at the GSA Specification Unit (WFSIS), Room 6039, 7th and D Streets S.W., Washington, D.C. 20407; telephone (202) 472-2205. Please call in advance for pickup service.