BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE DIRECTORY 33-303

1 FEBRUARY 2002

Communications and Information

COMPENDIUM OF COMMUNICATIONS AND INFORMATION TERMINOLOGY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://afpubs.hq.af.mil.**

OPR: HQ AFCA/ITPP (Mr. Johan Dekker)

Certified by: HQ USAF/SCXX (Mr. James Hundley)

Supersedes AFDIR 33-303, 1 November 1999.

Pages: 223

Distribution: F

This Air Force directory (AFDIR) implements Air Force Policy Directive (AFPD) 33-1, *Command, Control, Communications, and Computer (C4) Systems*; AFPD 33-2, *Information Protection* (will become Information Assurance); and AFPD 37-1, *Air Force Information Management* (will become AFPD 33-3). It identifies abbreviations, acronyms, and terminology most commonly used by the Air Force communications and information, and information assurance (IA) communities. It is not all encompassing, but will assist the user in researching unfamiliar terms. Use this directory as a source document when a standard communications or information-related acronym or definition is needed. Send recommended changes or comments to HQ AFCA/ITPP, 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222, through appropriate channels, using Air Force Form 847, **Recommendation for Change of Publication**.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

This revision updates the 1 Nov 99 version of this AFDIR; it adds, changes, and deletes abbreviations, acronyms, terms and definitions. Over 600 items were changed, deleted, or replaced; new items were added in the satellite, radar, navigational aids (NAVAIDS), and maintenance areas. The former Part I, Communications and Information, and Part II, Information Assurance, were combined for ease of reference and review.

1. Introduction . There are a number of different glossaries and other documents published within the Federal government, Department of Defense (DoD), and the Air Force that list communications and information terms and definitions. This directory is designed to help minimize the differences and conflicts between communications and information and IA terms, standardize them as much as possible, and reduce unnecessary proliferation.

2. Scope . The focus of this compendium is on communications and information, and IA terms, not on general-purpose Air Force or major command (MAJCOM) unique terms. MAJCOMs may supplement abbreviations, acronyms, and terms specific to their commands. **Attachment 1** contains communications and information, and IA abbreviations, acronyms, and terminology. As a general guideline, with few exceptions, the following items are not included: Air Force organizations and descriptions of their missions and functions; names and descriptions of Joint, DoD, or Air Force management programs or projects; functions, job titles, and their descriptions; communications systems/equipment nomenclatures and descriptions; computer software programs, and items containing commercial product names, trade names, or logos.

JOHN L. WOODWARD, JR, Lt General, USAF
DCS/Communications and Information

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

Abbreviations and Acronyms

A/D—Analog-to-Digital

A/G—Air-to-Ground (Communications)

A/N—Alphanumeric

AAA—Authentication, Authorization, and Accounting

AAL—Asynchronous Transfer Mode (ATM) Adaptation Layer

ABSS—Automated Base Supply System

ACE—1. Adaptive Communications Element
2. Automatic Clutter Eliminator

ACF—Automatic Clutter Filter

ACL—Access Control List

ACM—Access Control Mechanism

ACN—1. Accreditation Control Number
2. Airborne Communications Node

ACO—Access Control Officer

ACOT—Advanced Communications Officer Training

ACP—1. Allied Communications Publication
2. Associated Control Protocol
3. Automatic Communications Processor
4. Azimuth Change Pulse

ACS—Adaptive Computing System

ACSU—Advanced Channel Service Unit

ACT—Applied Computer Telephony

ACTD—Advanced Concept Technology Demonstration

ACTS—Automated Circuit Testing System

ACU—Automatic Calling Unit

ADC—Analog to Digital Converter

ADCCP—Advanced Data Communication Control Procedures

ADCON—Administrative Control

ADENS—Advanced Data Exchange Network System

ADFS—Automated Digital Facsimile System

ADL—Automatic Data Link

ADM—1. Add-Drop Multiplexers
2. Advanced Development Model

ADMS—Automatic Digital Message Switch

ADN—1. Advanced Digital Network
2. Agency Disclosure Notice

ADNX—Analog/Digital Network Exchange

ADP—Automated Data Processing

ADPCM—Adaptive Differential Pulse Code Modulation

ADPE—Automated Data Processing Equipment

ADPF—Automated Data Processing Facility

ADPRMIS—Automated Data Processing Resource Management Information System

ADPS—Automated Data Processing System

ADPSEC—Automated Data Processing Security

ADPSO—Automated Data Processing Selection Office

ADRSS—Automated Data Reports Submission System

ADS—Automated Data System

ADSL—Asymmetric Digital Subscriber Line

ADU—Accumulation and Distribution Unit

ADWS—Automated Digital Weather Switch

AE—Application Entity

AEHF—Advanced Extremely High Frequency

AEOS—Advanced Electro-Optical System

AES—Advanced Encryption Standard

AFADPP—Air Force Automated Data Processing Plan

AF—Audio Frequency

AF-CIO—Air Force Chief Information Officer

AFC—1. Area Frequency Coordinator
2. Automatic Frequency Control

AFCAT—Air Force Catalog

AFCDAd—Air Force Component Data Administrator

AFCDD—Air Force Corporate Data Dictionary

AFCERT—Air Force Computer Emergency Response Team

AFCISP—Air Force Communications and Information Strategic Plan

AFCVIL—Air Force Central Visual Information Library

AFD—Automated File Designator

AFDD—1. Air Force Doctrine Document
2. Air Force Data Dictionary

AFDE—Air Force Data Encyclopedia

AFDIR—Air Force Directory

AFDSEC—Air Force Data Systems Evaluation Center

AFDSRS—Air Force Defense Software Repository System

AFEKMS—Air Force Electronic Key Management System

AFEPL—Air Force Electronic Publishing Library

AFETS—Air Force Engineering and Technical Services

AFFORMS—Air Force Forms

AFH—Air Force Handbook

AFI—Air Force Instruction

AFIMS—Air Force Information Management System

AFINTNET—Air Force Intelligence Network

AFIRDS—Air Force Information Resources Dictionary System

AFIS—American Forces Information Service

AFIWC—Air Force Information Warfare Center

AFJI—Air Force Joint Instruction

AFMAN—Air Force Manual

AFMQCC—Air Force Maintenance Quality Control Checksheet

AFMD—Air Force Mission Directive

AFNCC—Air Force Network Control Center

AFNET—Air Force Network

AFNMS—Air Force Network Management System

AFNOC—Air Force Network Operations Center

AFOLDS—Air Force On-Line Data System

AFPAM—Air Force Pamphlet

AFPD—Air Force Policy Directive

AFPDC—Air Force Publishing Distribution Center

AFRSN—Air Force RED Switch Network

AFRTS—Armed Forces Radio and Television Service

AFSATCOM—Air Force Satellite Communications System

AFSCF—Air Force Satellite Control Facility

AFSCN—Air Force Satellite Control Network

AFSIR—Air Force Spectrum Interference Resolution

AFSN—Air Force Systems Networking

AFSPOC—Air Force Space Operations Center

AFT—Asynchronous File Transfer

AFTO—Air Force Technical Order

AGC—Automatic Gain Control

AGL—1. Above Ground Level
2. Air to Ground Laser

AHF—Adaptive High Frequency

AI—Artificial Intelligence

AIG—Address Indicator Group

AIMS—Automated Information Management System

AIN—Advanced Intelligence Network

AIRK—Area Interswitch Rekeying Key

AIS—Automated Information System

AISARC—Automated Information Systems Acquisition Review Council

AISS—Automated Information System Security

AIT—Automated Identification Technology

AITI—Automated Interchange of Technical Information

AJ—Anti-Jam

AK—Automatic Remote Rekeying

AKD/RCU—Automatic Key Distribution/Rekeying Control Unit

AKDC—Automatic Key Distribution Center

AKMC—Automated Key Management Center

AKMS—Automated Key Management System

ALC—Accounting Legend Code

ALE—Automatic Link Establishment

ALG—Application Layer Gateway

ALGOL—Algorithmic Language

ALN—Access Location Number

ALOC—Air Lines of Communication

ALTA—Advanced Lightweight Tactical Antenna

AM—Amplitude Modulation

AMA—Automatic Message Accounting

AMD—Advanced Micro Devices

AME—Antenna-Mounted Electronics

AMI—Alternate Mark Inversion

AMPS—Advanced Mobile Phone Service

AMS—1. Auto-Manual System
2. Autonomous Message Switch

AMSDS—Automated Management Supporting Data System

AMT—Aerial Mail Terminal

ANDVT—Advanced Narrowband Digital Voice Terminal

ANSI—American National Standards Institute

AO—1. Authorized Outage
2. Area of Operations

AOSS—Automated Office Support Systems

AP—1. Application Profile
2. Application Protocol
3. Anomalous Propagation

APC—Adaptive Predictive Coding

APF—Automated Processing Format

API—Application Programming Interface

APL—Assessed Products Listing

APPC—Advanced Program-to-Program Communication

APS—Automatic Protection Switching

APU—Auxiliary Power Unit

ARM—Agency Records Manager

ARP—1. Address Resolution Protocol
2. Azimuth Reference Pulse

ARS—Alaska Radar System

ARSR—Air Route Surveillance Radar

ARSTU—Auto Remote Secure Terminal Unit

ARTCC—Air Route Traffic Control Center

ARTS—Automated Radar Terminal System

ARU—Antenna Reference Unit

ASAT—Antisatellite

ASCII—American Standard Code for Information Interchange

ASCT—Auxiliary Satellite Control Terminal

ASCV—Annular Subclutter Visibility

ASD(C3I)—Assistant Secretary of Defense for Command, Control, Communications and Intelligence (C3I)

ASG—Architecture Steering Group

ASIC—Application Specific Integrated Circuit

ASIM—Automated Security Incident Measurement

ASIT—Adaptive Surface Interface Terminal

ASM—Administrative Support Manual

ASNC—Alternate SATCOM Network Controller

ASPJ—Advanced Self-Protection Jammer

ASR—Airport Surveillance Radar

ASSA—Automated Support Systems Architecture

ASSIST—Automated information system Security Incident Support Team

ASU—Approval for Service Use

ATAM—Automated Threat Assessment Methodology

ATTAPI—Attachment Packet Interface

ATC—Air Traffic Control

ATD—Advanced Technology Demonstration

ATDM—Asynchronous Time-Division Multiplexing

ATE—1. Asynchronous Terminal
2. Automated Test Equipment

ATM—Asynchronous Transfer Mode

ATN—Air Technology Network

ATS—Advanced Tracking System

ATW—Analog Trunked Wideband

AV—Audiovisual

AVD—Alternate Voice Data

AVR—1. Alternate Voice Record
2. Advanced VLF/LF Receiver

AWP—Awaiting Parts

AWS—Advanced Wideband Satellite

AZ—Azimuth

B—1. Bell
2. Byte

B2B—Business-to-Business

BAM—Basic Access Module

BASIC—Beginners All-Purpose Symbolic Instruction Code

BBP—Baseband Processor

BBS—Bulletin Board Service (System)

BBTC—Broadband Video Teleconferencing

BCB—Broadband Communications Bus

BCC—Backup Channel Controller

BCI—Bit Count Integrity

BCL—Binary Cutter Location

BCLD—Binary Cutter Location Data

BCRDR—Bar Code Reader

BCS—Baseband Communications System

BCSA—Base-Level Communications-Computer Systems Assessment

BCST—Beacon Sort Code

BCUS—Basic Computer User Skills

BDC—Backup Domain Controller

BDN—Bulk Data Network

BDS—1. Base Distribution System
2. Broadband Distribution System

BER—Bit Error Ratio

BERT—Bit Error Ratio Test

BERTS—Bit Error Ratio Test Set

BEXR—Beacon Extractor Recorder

BFTA—Beacon False Target Analysis

BIAO—Base Information Assurance Officer

BII—Base Information Infrastructure

BioAPI—Biometrics Application Programming Interface

BIOS—Basic Input/Output System

BIP—Base Information Protection

BISDN—Broadband Integrated Services Digital Network

bit—Binary Digit

BIST—Built-in Self-Test

BIT—Built-In Test

BITC—Base Information Transfer Center

BITE—Built-in Test Equipment

BITS—Base Information Transfer System

BIU—Bus Interface Unit

BLOB—Binary Large Object

BLOS—Beyond Line-of-Sight

BLSR—Bi-directional Line Switched Ring

BMH—Base Message Host

BMTA—Backbone Message Transfer Agent

BOD—Business Object Document

BOM—Bit-Oriented Message

BOSS—Basic Operating System Software

BPAC—Budget Program Activity Code

BPID—Blueprint Phased Implementation Directive

BPS—Bits Per Second

BPSK—Binary Phase Shift Keying

BRI—Basic Rate Interface

BSC—Binary Synchronous Communications

BSFT—Byte Stream File Transfer

BSHR—Bi-directional Self-Healing Ring

BSR—Blip Scan Ratio

BSS—Base Switching System

BTC—Base Telecommunications Center

BTS—Base Telephone System

BVR—Beyond Visual Range

BW—1. Bandwidth
2. Beam Width

C&A—Certification and Accreditation

C2—Command and Control

C2IPS—Command and Control Information Processing System

C3—Command, Control, and Communications

C3I—Command, Control, Communications, and Intelligence

C4—Command, Control, Communications, and Computers

C4I—Command, Control, Communications, Computers, and Intelligence

C4ISP—Command, Control, Communications, Computers, and Intelligence Support Plan

C4ISR—Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance

CA—1. Controlling Authority
2. Cryptanalysis
3. COMSEC Account
4. Command Authority
5. Certification Authority

CAA—Controlled Access Area

CAD—Computer-Aided Design

CAE—1. Computer-Aided Engineering
2. Common Applications Environment

CAI—Computer-Aided Instruction

CALCE—Computer-Aided Life-Cycle Engineering

CALS—Computer-Aided Logistics Support

CAM—Computer-Aided Manufacturing

CAMS—Core Automated Maintenance System

CAN—Campus Area Network

CANDI—Commercial And Non-Developmental Item

CAP—1. Controlled Access Protection
2. Cryptographic Access Program

CAPI—Cryptographic Application Program Interface

CAR—Customer Account Representative

CARDS—Comprehensive Approach to Reusable Defense Software

CASE—Computer-Aided System Engineering

CAST—Computer-Aided Software Testing

CAT—1. Cable and Antenna Team
2. Computer-Aided Testing

CATV—Cable Television

CAW—Certificate Authority Workstation

CBCS—Common Baseline Circuit Switch

CBCSS—Combat Communications Support Squadron

CBEFF—Common Biometric Exchange File Format

CBI—Computer-Based Instruction

CBR—Constant Bit Rate

CBRN—Caribbean Basin Radar network

CBT—1. Computer-Based Training
2. CSP Backside Terminal

CBU—Conference Bridge Unit

CC—1. Common Carrier
2. Channel Controller
3. Communications Center
4. Common Criteria

CCA—1. Circuit Card Assembly
2. Clinger-Cohen Act

CCB—Configuration Control Board

CCC—Communications Common Carrier

CCD—Charge Coupled Device

CCE—Contingency Communications Element

CCEB—Combined Communications-Electronics Board

CCEP—Commercial COMSEC Endorsement Program

CCF—Consolidated Computer Facility

CCI—Controlled Cryptographic Item

CCIRC—CONUS Cable Installation Requirements Contract

CCIS—Common Center Interswitch Signaling

CCITT—Consulting Committee on International Telephone and Telegraph

CCM—Counter-Countermeasure

CCO—Commercial Communications Office

CCOW—Channel Control Orderwire

CCP—Contingency Communications Package

CCPS—Contingency Communications Parent Switch

CCS—1. Command and Control System
2. Constellation Control Station
3. Common Channel Signaling

CCSD—Command Communications Service Designator

CCTV—Closed Circuit Television

CCWO—Commercial Communications Work Order

CD—Compact Disk

CDA—Central Design Activity

CDAd—Component Data Administrator

CDBS—Common Data Base System

CDE—Common Desktop Environment

CD-I—Compact Disk Interactive

CDI—Conditioned Diphase

CDL—Common Data Link

CDM—Clear Day Map

CDMA—Code Division Multiple Access

CDMGB—Cable Driver Modem Group Buffer

CDN—Compressed Dial Number

CDOCS—Contingency DSCS Operations Control System

CDPD—Cellular Digital Packet Data

CDRL—Contractor Data Requirements List

CD-R—Compact Disk-Recordable

CDR—1. Combat Deployable Radio
2. Critical Design Review

CD-ROM—Compact Disk-Read-Only Memory

CD-RW—Compact Disk-Re-writeable

CDS—1. Cryptographic Device Services
2. Compact Digital Switch

CDV—Compressed Digital Video

CD-V—Compact Disk-Video

CD-WO—Compact Disk-Write Once

CD-WORM—Compact Disk-Write Once-Read Many

CD-XA—Compact Disk-Extended Architecture

C-E—Communications-Electronics

CE—Compromising Emanations

CEC—Cooperative Engagement Capability

CEF—Common Equipment Facility

CEG—Common Equipment Group

CELP—Codebook Excited Linear Predictive Coding

CEM—1. Communications-Electronics Maintenance
2. Control Electronics Module

CEMI—Communications-Electronics Maintenance Instruction

CEOI—Communications-Electronics Operating Instruction

CENTREX—Central Exchange

CEPR—Compromising Emanation Performance Requirement

CER—1. Cryptographic Equipment Room
2. Character Error Rate

CERT—Computer Emergency Response Team

CFAR—Constant False Alarm Rate

CFD—Common Fill Device

CFE—Contractor Furnished Equipment

CFEP—Communications Front End Processor

CFM—Computer Facility Manager

CFR—Code of Federal Regulations

CG—Communications Group

CGA—Color Graphics Adapter (or Array)

CGI—1. Computer Graphics Interface
2. Common Gateway Interface

CGM—Computer Graphics Metafile

CGP—Common Graphics Package

CGS—Common Ground Station

Ch—Channel

CHAT—Conversational Hypertext Access Technology

CHPS—Characters Per Second

CHS—Common Hardware and Software

CI—1. Counterintelligence
2. Counterinformation
3. Critical Information

CIAC—Computer Incident Assessment Capability

CIDE—Communications Interfaces and Data Exchange

CIFS—Common Internet File System

CIK—Crypto-Ignition Key

CIM—1. Communications Improvement Memorandum
2. Crypto Interface Module

CIO—Chief Information Officer

CIP—1. Critical Infrastructure Protection
2. Crypto-Ignition Plug

CIRK—Common Interswitch Rekeying Key

CIRT—Computer Incident Response Team

CIRT—Computer Security Incident Response Team

CITS—Combat Information Transfer System

CK—Compartment Key

CKG—Cooperative Key Generation

CKL—Comprised Key List

CL—Certification Level

CLEC—Competitive Local Exchange Carrier

CLMD—COMSEC Local Management Device

CLNP—Connectionless Network Protocol

CLNS—Connectionless Network Service

CLS—Contractor Logistics Support

CLT—Communications Line Terminal

CLTP—Connectionless Transport Protocol

CLTS—Connectionless Transport Service

CM—1. Configuration Management
2. Countermeasure
3. Crypto Module
4. Content Management

CMA—Control, Monitor, and Alarm

CMCS—COMSEC Material Control System

CMI—Computer-Managed Instruction

CMIP—Common Management Information Protocol

CMIS—Common Management Information Services

CMIS/P—Common Management Information Service and Protocol

CMM—Capability Maturity Model

CMO—Circuit Management Office

CMOS—Complimentary Metal-Oxide Semiconductor

CMP—Configuration Management Plan

CMU—Control and Matrix Unit

CN—Communications Network

CNA—Computer Network Attack

CNCE—Communications Nodal Control Element

CNCS—Cryptonet Control Station

CND—Computer Network Defense

CNE—Computer Network Exploitation

CNIN—Composite Network Front End Internal Network

CNK—Cryptonet Key

CNR—Combat Net Radio

CNRI—Combat Net Radio Interface

CNWDI—Critical Nuclear Weapon Design Information

CO—Central Office

COB—Collocated Operating Base

COBOL—Common Business Oriented Language

CODEC—Coder-Decoder

COE—Common Operating Environment

COHO—Coherent Oscillator

COM—Computer Output Microform

COMCAM—Combat Camera

COMJAM—Communications Jamming

COMM—Communications

COMPUSEC—Computer Security

COMSAT—Communications Satellite

COMSATCOM—Commercial Satellite Communications

COMSEC—Communications Security

CoN—Certificate of Networthiness

CONOPS—Concept of Operations

CONPLAN—Contingency Plan

COPS—Computer Oracle Password and Security

COR—Central Office of Record (COMSEC)

CORBA—Common Object Request Broker Architecture

COS—Class of Service

COTS—Commercial-Off-the-Shelf

CP—Communications Processor

CPACS—Coded Pulse Anti-Clutter System

CP/M—Computer Program/Microprocessor

CPC—1. Communications Payload Controller
2. Computer Program Component
3. Cross-Platform Communications

CPE—Customer Premise Equipment

CPCI—Computer Program Configuration Item

CPI—Critical Program Information

CPIWI—Customer Premise Inside Wire Installation

CPM—1. Computer Performance Measurement
2. Continuous Phase Modulation

CPMF—Computer Program Maintenance Facility

CPS—COMSEC Parent Switch

CP-SS—Central Processor Subsystem

CPU—Central Processing Unit

CRC—Cycle Redundancy Check

CRD—Capstone Requirements Document

CRI—Collective Routing Indicator

CRL—Certificate Revocation List

CRLCMP—Computer Resources Life Cycle Management Plan

CRM—Command Records Manager

CRMA—Cyclic Reservation Multiple Access

CRP—COMSEC Resources Program

CRT—Cathode Ray Tube

CRU—Computer Resource Utilization

CRWG—Computer Resources Working Group

Crypt/Crypto—Cryptographic-Related

CS—Communications Squadron

CSA—1. Cognizant Security Authority
2. Communications Service Authorization

CSB—Computer Support Base

CSC—1. Computer Software Component
2. Customer Service Center

CSCD—Cellular Switched-Circuit Data

CSCI—1. Commercial Satellite Communications Initiatives
2. Common Utilities Computer Software Configuration
3. Computer Software Configuration Item

CSCLS—Computational Support for Create Logistics Research

CSE—1. Communications Security Element
2. Common Support Equipment

CSET—Computer Security Engineering Team

CSIR—Communications Systems Installation Record

CSM—Computer Systems Manager

CSMA—Carrier Sense Multiple Access

CSMA/CA—Carrier Sense Multiple Access/Collision Avoidance

CSMA/CD—Carrier Sense Multiple Access/Collision Detection

CSO—Communications and Information Systems Officer

CSOM—Computer Systems Operator’s Manual

CSP—Communications Support/System Processor

CSPMD—Call Service Position Modem

CSR—Cell Switch Router

CSS—1. COMSEC Subordinate Switch
2. Constant Surveillance Service
3. Continuous Signature Service
4. Coded Switch System

CSSO—1. Computer Systems Security Officer
2. Contractor Special Security Officer

CSSP—Computer Security Support Program

CSTVRP—Computer Security Technical Vulnerability Reporting Program

CSU—1. Channel Service Unit
2. Communications Switching Unit
3. Computer Software Unit

CSU/DSU—Channel Service Unit/Data Service Unit

CT—Cellular Telephone

CT&E—Certification Test and Evaluation

CTAK—Cipher Text Auto-Key

CTC—Combat Theater Communications

CTD—Common Tactical Dataset

CTI—Computer Telephony Integration

CTIS—1. Command Tactical Information System
2. Commander's Theater Information System

CTMC—Communications Terminal Module Controller

CTO—Certificate to Operate

CTS—1. Clear-to-Send
2. Communications Technology Service
3. Conversation Time Sharing

CTTA—Certified Tempest Technical Authority

CUA—Common User Access

CUI—Common User Interface

CUP—Communications Security Utility Program

CVC—Consonant-Vowel-Consonant

CVSD—Continuously Variable Sloped Delta

CW—Continuous Wave

D/A—Digital-to-Analog

DA—Data Administrator

DAA—Designated Approving Authority

DAC—Digital-to-Analog Converter

DAC—Discretionary Access Control

DAd—Data Administrator

DAL—Data Accessions List

DAMA—Demand Assigned Multiple Access

DAP—1. Data Automation Proposal, Panel, or Plan
2. Document Application Profile

DAPM—Data Administration Program Manager

DAPMO—Data Administration Program Management Office

DASA—Demand Assigned Single Access

DASP—Data Administration Strategic Plan

DASR—Digital Airport Surveillance Radar

DAT—Digital Audio Tape

DAVIS—Defense Automated Visual Information System

DB—Data Base

dB—Decibel

DBA—Dynamic Bandwidth Allocation

DBD—Display Bypass and Duplication

dBj—Decibel, referenced to 1 Joule

dBm—Decibel, referenced to 1 milliwatt

DBMD—Data base Meta Dictionary

DBR—Display Bypass Reception

DBS—Direct Broadcast Satellite

dBsm—Decibel, referenced to 1 square meter

DBT—Data Base Transfer

dBW—Decibel, referenced to 1 Watt

DC—1. Direct Current
2. Down Converter
3. Data Communication
4. Duty Cycle
5. Differential Correction

DCA—Distribution Communications Architecture

DCC—Data Communications Channel

DCE—Data Circuit Equipment (Modem)

DCGS—Distributed Common Ground System

DCI—1. Defensive Counterinformation
2. Data Channel Interface

DCM—Data Communications Module

DCN—1. Design Change Notice

2. Digital Conventional Narrowband

DCO—Dial Central Office

DCP—Data Communications Processor

DCPS—Data Communications Protocol Standards

DCRSI—Digital Cassette Recording System, Incremental

DCS—Digital Communications System

DCT—Data Communications Terminal

DCTE—Data Circuit Terminating Equipment

DCTN—Defense Commercial Telecommunications Network

DD—1. Data Dictionary
2. Department of Defense (*designated forms only*)

DDCS—Data Distribution Communications System

DDD—1. Data Description Document
2. Direct Distance Dialing

DDDS—Defense Data Dictionary System

DDE—Direct Data Exchange

DDF—Data Descriptive File

DDMA—Disk Directory Memory Access

DDN—Defense Data Network

DDP—1. Distributed Data Processing
2. Digital Data Processor

DDRS—Defense Data Repository System

DDS—Digital Data Service

DDT&E—Design, Development, Test, and Evaluation

DDU—Digital Distribution Unit

DEA—Data Encryption Algorithm

DEB—Digital European Backbone

DED—Data Element Dictionary

DEMUX—Demultiplexer

DEQPSK—Differentially Encoded Quadrature Phase Shift Keying

DES—1. Data Element Standardization
2. Data Encryption Standard

DFT—Digital Fourier Transform

DGM—Digital Group Multiplexer

DGSA—Defense Goal Security Architecture

DHCP—Dynamic Host Configuration Protocol

DI—Data Integrity

DIAP—Defense-Wide Information Assurance Program

DIB—Data Information Base

DIC—Document Identifier Code

DID—1. Data Item Description
2. Direct Inward Dialing

DIF—Digital Interface

DII—Defense Information Infrastructure

DIICC—Defense Information Infrastructure Control Concept

DII/COE—Defense Information Infrastructure/Common Operating Environment

DIMM—Digital In-line Memory Module

DIO—Defense Information Operations

DISA—1. Defense Information Systems Agency
2. Data Interchange Standards Association

DISAN—Defense Information Systems Agency Notice

DISANET—Defense Information System Agency Information Network

DISN—Defense Information Systems Network

DISNET—Defense Integrated Secure Network

DISS—Digital Ionospheric Sounding System

DIT—Directory Information Tree

DITCO—Defense Information Technology Contracting Office

DITPRO—Defense Information Technology Procurement Office

DITS—Digital Imagery Transmission System

DITSCAP—DoD Information Technology Security Certification and Accreditation Process

DITSO—Defense Information Technology Services Organization

DIU—Data Interface Unit

DL—Distance Learning

DLED—Dedicated Loop Encryption Device

DLT—Decision Logic Table

DM—Domain Manager

DMA—Direct Memory Access

DMATS—Defense Metropolitan Area Telephone Service/System

DMC—Defense Megacenter

DME—Distance Measuring Equipment

DMS—Defense Message System

DMTI—Digital Moving Target Indicator

DNS—1. Data Network System
2. Domain Name System

DNVT—Digital Nonsecure Voice Terminal

DoD TCSEC—Department of Defense Trusted Computer System Evaluation Criteria

DOD—Direct Outward Dialing

DOS—Disk Operating System

DOV—Data Over Voice

DOW—Digital Orderwire

DP—Dial Pulse

DP&D—Data Processing and Display

DPA—Dual Phone Adapter

DPAS—Digital Patch and Access System

DPBX—Digital Private Branch Exchange

DPC—Data Processing Center

DPI—1. Data Processing Installation
2. Dots Per Inch

DPL—1. Degausser Products List
2. Diode-Pumped Laser

DPM—Dual Phone Modem

DPN—Digital Pipeline Network

DPS—Defense Printing Service

DPSK—Differential Phase Shift Keying

DRAM—Dynamic Random Access Memory

DRFM—Digital Radio Frequency Memory

DRSN—Defense Red Switch Network

DS—1. Digital Signature
2. Digital Switch

DSA—1. Digital Signature Algorithm
2. Directory Service Agent

DSAD—Data Systems Authorization Directory

DSB—Digital in-band trunk Signalling Buffer

DSC—DISN Service Center

DSCS—Defense Satellite Communications System

DSCSOC—Defense Satellite Communications System Operations Center

DSD—Data System Designator

DSDO—Data Systems Design Office

DSL—Digital Subscriber Line

DSM—Digital Switching Module

DSN—Defense Switched Network

DSNET—Defense Secure Network

DSP—Digital Signal Processor

DSR—Data Set Ready

DSRS—Defense Software Repository System

DSS—1. Digital Switching System
2. DISN Switched Services

DSSO—Data System Support Office

DSTE—Digital Subscriber Terminal Equipment

DSU—1. Data Service Unit
2. Digital Service Unit

DSVT—Digital Subscriber Voice Terminal

DT—Dial Tone

DT&E—Development, Test, and Evaluation

DTC—1. Data Transfer Cartridge
2. Digital Technical Control

DTD—1. Data Transfer Device
2. Document Type Definition

DTE—1. Data Terminal Equipment
2. Digital Target Extractor

DTED—Digital Terrain Elevation Data

DTG—1. Date-Time-Group
2. Digital Transmission Group
3. Digital Trunk Group

DTI—Digitized Technical Information

DTIC—Defense Technical Information Center

DTLS—Descriptive Top-Level Specification

DTM—Data Transfer Module

DTMF—Dual Tone Multiple Frequency

DTMI—Digital Moving Target Indicator

DTN—Data Transmission Network

DTP—Desktop Publishing

DTR—Data Terminal Ready

DTS—1. Data Terminal Set
2. Diplomatic Telecommunications Service

DTS-C—DISN Transmission Services - CONUS

DTVTC—Desktop Video Teleconferencing

DUA—Directory User Agent

DUI—Data Use Identifier

DVD—1. Digital Versatile Disk
2. Digital Video Disk

DVD-R—Digital Versatile Disk - Recordable

DVD-ROM—Digital Versatile Disk - Read-Only Memory

DVD-RW—Digital Versatile Disk - Re-Writeable

DVI—1. Digital Video Interactive
2. Digital Video Instruction

DVOW—Digital Voice Orderwire

DVRS—Digital Voice Recorder System

DVS-G—DISN Video Services - Global

DWDM—Dense Wavelength Division Multiplexing

DX—Distance

E3—Electromagnetic Environmental Effects

E&I—Engineering and Installation

EA—1. Electronic Attack
2. Environmental Assessment

EAID—Equipment Authorization Inventory Data

EAM—1. Emergency Action Message
2. Electroabsorbtion Modulator

EAM—Emergency Action Message

EAPROM—Electrically Alterable Programmable Read-Only Memory

EAROM—Electrically Alterable Read-Only Memory

EARTS—Enroute Automated Radar Tracking System

EB/EC—Electronic Business/Electronic Commerce

EBB—Electronic Bulletin Board

EBCDIC—Extended Binary Coded Decimal Interchange Code

EBO—Electronic Business Operations

EC—1. Electronic Combat
2. Electronic Commerce
3. Echo Canceller
4. Earth Coverage

EC/EDI—Electronic Commerce/Electronic Data Interchange

ECAD—Electronic Computer-Aided Design

ECC—Error Correction Code

ECCM—1. Electronic Counter-Countermeasure
2. Error Correcting Code Memory

ECM—Electronic Countermeasures

ECN—Engineering Change Notice

ECO—Engineering Change Order

ECP—1. Engineering Change Proposal
2. Extended Capability Port

ECPL—Endorsed Cryptographic Products List (a section in the *Information Systems Security Products and Services Catalogue*)

ECR—Engineering Change Request

EDAC—Error Detection and Correction

EDESPL—Endorsed Data Encryption Standard Products List

EDI—Electronic Data Interchange

EDIFACT—Electronic Data Interchange for Administration, Commerce, and Transport

EDITS—Enhanced Digital Imagery Transmission System

EDM—Engineering Development Model

EDMS—Electronic Document Management System

EDO—Extended Data Out

EDP—Electronic Data Processing

EDS—Electronic Data Systems

EEFI—Essential Elements of Friendly Information

EEI—1. Essential Elements of Information
2. External Environment Interface

EEPROM—Electrically Erasable Programmable Read-Only Memory

EF—Electronic Form

EFD—Electronic Fill Device

EFT—Electronic Funds Transfer

EFTO—Encrypt For Transmission Only

EGA—Enhanced Graphics Adapter

EGADS—Electronic Generation, Accounting, and Distribution System

EGP—Extended Gateway Protocol

EHDC—EMP Hardened Dispersal Communications

EHF—Extremely High Frequency

EHFASS—Extremely High Frequency Antenna Support System

EHz—Exahertz

EI—Engineering and Installation

EIA—Electronics Industry Association

EIDE—Enhanced Integrated Drive Electronics

EIM—Enterprise Information Management

EIRP—Effective Isotropic Radiated Power

EISA—Extended Industry Standard Architecture

EKDD—Electronic Key Distribution Device

EKMS—Electronic Key Management System

EL—Elevation

ELF—Extremely Low Frequency

ELINT—Electronic Intelligence

ELSCAN—Elevation Scan

ELSEC—Electronic Security

EMC—1. Electromagnetic Compatibility
2. Emergency Message Change

EMCON—Emission Control

EMG—Enhanced Multinet Gateway

EMI—Electromagnetic Interference

EMP—Electromagnetic Pulse

EMR—Electromagnetic Radiation

EMRH—Electromagnetic Radiation Hazards

EMS—1. Electronic Message System
2. Extended Memory Specification

EMSEC—Emission Security

EMSS—1. Electronic Matrix Switching System
2. Enhanced Mobile Satellite Service

ENTAC—Entrance National Agency Check

ETVS—Enhanced Terminal Voice Switch

EO—1. Electro-Optical
2. Executive Order

EOD—1. End of Data
2. End of Dial

EOF—End-of-File

EO/IR—Electro-optical/Infrared

EP—Electronic Protection

EPBX—Electronic Private Branch Exchange

EPL—Evaluated Products List

EPP—Endpoint Printer

EPROM—Erasable Programmable Read-Only Memory

EPU—Emergency Power Unit

ERM—Electronic Records Management

ERP—Effective Radiated Power

ERTZ—Equipment Radiation Tempest Zone

ES—1. Electronic Warfare Support
2. End System

ESA—Emission Security Assessment

ESC—Emergency Status Code

ESD—1. Electrostatic Sensitive Device
2. Electrostatic Discharge

ESDI—Enhanced System Device Interface

ESMR—Enhanced Specialized Mobile Radio

ESP—Encapsulating Security Protocol

ESS—1. Electronic Switching System
2. Electronic Scoring Site

ET—Earth Terminal

ETADS—Enhanced Transmission Automated Data System

ETC—1. Earth Terminal Complex
2. Enhanced Terminal Communications

ETIC—Estimated Time in Commission

ETL—Endorsed Tools List

ETPL—Endorsed Tempest Products List Item

ETRO—Estimated Time of Return to Operation

ETS—Electronic Transaction System

ETVS—Enhanced Terminal Voice Switch

EU—Essential User

EUCI—Endorsed for Unclassified Cryptographic Information

EW—Electronic Warfare

EWS—Electronic Warfare Support

F—Functional Distribution

FAR—1. False Alarm Rate
2. False Acceptance Rate

FARM—Functional Area Records Manager

FAS—Functional Address Symbol

FAT—File Allocation Table

FAX—Facsimile

FBD—Formatted Binary Data

FBL—Functional Baseline

FCA—Functional Configuration Audit

FCC—Federal Communications Commission

FCO—1. Frequency Controlled Oscillator
2. Facility Control Office

FCS—Full Communications Service

FD—Fault Detection

FDDI—Fiber Distributed Data Interface

FDIU—Fill Device Interface Unit

FDMA—Frequency Division Multiple Access

FDX—Full Duplex

FEC—Forward Error Correction

FEP—Front End Processor

FET—Field Effect Transistor

FFT—Fast Fourier Transform

FI—Fault Isolation

FIFO—First-In First-Out

FILO—First-In Last-Out

FIP—Federal Information Processing

FIPS—Federal Information Processing Standard

FL—Flight Level

FLIR—Forward Looking Infrared

FLOPS—Floating Point Operations Per Second

FLTSATCOM—Fleet Satellite Communications

FM—Frequency Modulation

FMA—Frequency Management Algorithm

FMC—Fully Mission Capable

FO—1. Fiber Optics
2. Flash Override

FOC—Full Operational Capability

FOCI—Foreign Owned, Controlled, or Influenced

FOIA—Freedom of Information Act

FOL—Forward Operating Location

FOM—Fiber Optic Modem

FORTEZZA—PCMCIA card with National Security Agency (NSA) encryption algorithm

FORTRAN—Formula Translator

FOT—Fiber Optics Transceiver

FOT&E—Follow-On Test and Evaluation

FOTS—Fiber Optic Transmission System

FOUO—For Official Use Only

FOW—Forward Orderwire

FPGA—Field Programmable Gated Array

FPI—Functional Process Improvement

FQR—Formal Qualification Review

FQT—Formal Qualification Testing

FR—Federal Register

FRA—Federal Records Act

FRAM—Ferroelectric Random Access Memory

FRC—1. Federal Records Center
2. Frame Recovery Circuit

FRO—Frequency Reference Oscillator

FROST—Fast Read-out Optical Storage

FRR—False Rejection Rate

FRS—Family Radio Service

FS—File Server

FSA—Functional System Administrator

FSK—Frequency Shift Keying

FSRS—Functional Security Requirements Specification

FSTS—Federal Secure Telephone Service

FTAM—File Transfer Access Management

FTP—File Transfer Protocol

FTS—1. Federal Telecommunications System
2. File Transfer System

FWA—Four-Wire Adaptor

GAN—Global Area Network

Gb—Gigabit

GBR—Ground-Based Radar

GBS—Global Broadcast Services

Gbyte—Gigabyte

GCC—Global Control Center

GCCS—Global Command and Control System

GCSS—Global Combat Support System

GEO—Geosynchronous Earth Orbit

GEP—Ground Entry Point

GEPETE—General Purpose Electronic Test Equipment

GFE—Government Furnished Equipment

GFI—Government Furnished Information

GFM—Government Furnished Material

GFP—Government Furnished Property

GFS—Government-Furnished Software

GHA—Greenwich Hour Angle

GHz—Gigahertz

GIF—Graphics Interchange Format

GIG—Global Information Grid

GII—Global Information Infrastructure

GILS—Government Information Locator Service

GIP—Ground Intercept Point

GIS—Geographical Information System

GK—Gate Keeper

GM—Group Modem

GMF—Ground Mobile Forces

GMPCS—Global Mobile Personal Communications System

GMT—1. Ground Multi-band Terminal
2. Greenwich Mean Time

GNIE—Global Network Information Enterprise

GOCO—Government-Owned Contractor-Operated

GOSIP—Government Open Systems Interconnection Profile

GOTS—Government-Off-The-Shelf

GPS—Global Positioning System

GRIB—Gridded Binary

GSM—Group Special Mobile (standard)

GSSC—Global SATCOM Support Center

G/T—Antenna Gain-to-System Noise Temperature Ratio

GTC—Gate Time Control

GTN—Global Transportation Network

GTS—Global Telecommunications Service

GUI—Graphical User Interface

GUPS—Giga Updates Per Second

GW—1. Gateway

2. Gigawatt

GWEN—Ground Wave Emergency Network

HAG—High Assurance Guard

HCI—1. Human Computer Interface|
2. Hardness Critical Item

HCL—High-Capacity Links

HDA—Head-Drive Assembly

HDBS—Host Data-base System

HDLC—High Level Data-Link Control

HDSL—High bit rate Digital Subscriber Line

HDTV—High Definition Television

HEL—High Energy Laser

HEMP—High Altitude Electromagnetic Pulse

HERO—Hazards of Electro-magnetic Radiation to Ordnance

HF—1. High Frequency
2. Height Finder

HF-ACP—High Frequency-Automated Communications Processor

HFRB—High Frequency Regional Broadcast

HFSSB—High Frequency Single Sideband

HGML—Hypertext Generalized Markup Language

HHD—Hand Held Device

HICS—Hardened Intersite Cable System

HIPPI—High Performance Parallel Interface

HIPRA—High Speed Digital Processor Architecture

HIRF—High Intensity Radiation Fields

HLI—Host Language Interface

HLL—High Level Language

HMA—High Memory Area

HMI—Human/Machine Interface

HNA—Host Nation Approval

HNCA—Host Nation Connection Approval

HOL—High Order Language

HPA—High Power Amplifier

HPM—High Power Microwave

HPSC—High Performance Scientific Computer

HPW—High Performance Workstation

HSFEC—High Speed Forward Error Correction

HSSI—High Speed Serial Interface Protocol

HTML—Hypertext Markup Language

HTTP—Hypertext Transfer Protocol

HUD—Heads Up Display

HUS—Hardened Unique Storage

HUSK—Hardened Unique Storage Key

HVPS—High Voltage Power Supply

HW—Hardware

HWRLP—Heavyweight Rotatable Log Periodic (antenna)

Hz—Hertz

I&A—Identification and Authentication

IA—Information Assurance

IACP—Improved Azimuth Change Pulse

IAS—Immediate Access Storage

IAT—Installation and Acceptance Test

IBAC—Identity Based Access Control

IBS—Integrated Broadcast System

IC—1. Integrated Circuit
2. Interim Change

IC2—Integrated Command and Control

ICAD—Integrated Computer-Aided Design

ICAP—Integrated Communications Access Package

I-CASE—Integrated Computer Aided Software Engineering

ICATS—Intermediate Capacity Automated Telecommunications System

ICB—Information Collection Budget

ICD—Installation Completion Date

ICDB—Integrated Communications Data Base

ICDCS—Integrated Control, Display, and Communications Subsystem

ICI—Interactive Communications Interface

ICR—Information Collections and Reports

ICS—Integrated Communications Switch

ICTP—Information Collection, Transfer, and Processing

ICU—Interface Control Unit

ICW—1. Interactive Courseware
2. Interrupted Continuous Wave

ID—Initial Distribution

IDA—Initial Denial Authority

IDB—1. Integrated Data Base
2. Intelligence Data Base

IDE—Integrated Drive Electronics

IDEF—Integrated Definition

IDF—Intermediate Distribution Frame

IDHS—Intelligence Data Handling System

IDM—Information Dissemination Management

IDN—Integrated Digital Network

IDNX—Integrated Digital Network Exchange

IDS—1. Integrated Data System
2. Intrusion Detection System

IDT—Intrusion Detection Tools

IDTS—Integrated Digital Telecommunications System

IE—Information Engineering

IEC—Inter-Exchange Carriers

IEEE—Institute for Electrical and Electronics Engineers

IEMATS—Improved Emergency Message Automatic Transmission System

IEO—International Exchange Office

IER—Information Exchange Requirement

IESS—Integrated Electromagnetic System Simulator

IETM—Interactive Electronic Technical Manual

IF—Intermediate Frequency

IFFN—Identification, Friend, Foe, or Neutral

IIR—Imaging Infrared

IIRK—Interarea Interswitch Rekeying Key

IIW—Information-In-Warfare

IJAVA—Inverse Jamming Amplitude Versus Azimuth

IKE—Internet Key Exchange

ILS—1. Integrated Logistics Support
2. Instrument Landing System

ILSP—Integrated Logistics Support Plan

IM—Information Management

IMINT—Imagery Intelligence

IMP—Interface Message Processor

IMS—Information Management System

IMU—Intermediate Message Unit

IMUX—Intelligent Multiplexer

INE—In-Line Network Encryptor

INFOSEC—Information Systems Security

INMARSAT—International Maritime Satellite Terminal

INP—Intelligent Network Processor

INTELSAT—International Telecommunications Satellite (Organization)

IO—1. Information Operations
2. Indian Ocean (area footprint)

IOC—Initial Operating Capability

IOE—Input and Output Extender

IOP—Input/Output Processor

IOT&E—Initial Operational Test and Evaluation

IP—Internet Protocol

IPA—Intermediate Power Amplifier

IPAP—Information Protection Assessment Program

IPAT—Information Protection Assessment and Assistance Team

IPC—Information Processing Center

IPE—Information Processing Equipment

IPM—1. Impulses Per Minute
2. Interpersonal Messaging

IPMS—Information Processing Management System

IPO—Information Protection Operations

IPS—Information Processing System

IPSEC—Secure Internet Protocol

IPSO—Internet Protocol Security Option

IPT—Integrated Product Team

IPTP—Interoperability Policy and Test Panel

IPU—Integrated Power Unit

IR—Infrared

IRAD—Independent Research and Development

IRCM—Infrared Countermeasures

IRID—Incident Report Identification

IRK—Interswitch Rekeying Key

IRM—Information Resource Management

IRQ—Interrupt Request

IRRM—Information Reports Requirements Manager

IS—1. Information System
2. Information Superiority

ISA—Industry Standard Architecture

ISAR—Inverse Synthetic Aperture Radar

ISB—Independent Side Band

ISD—1. Information Systems Directive
2. Installation Start Date

ISDN—Integrated Services Digital Network

ISLMR—Intrinsically Safe Land Mobile Radio

ISLS—Interrogator Side Lobe Suppression

ISO—International Standards Organization

ISOC—Internet Society

ISP—Internet Service Provider

ISR—1. Intra-Squad Radios
2. Intelligence, Surveillance, and Reconnaissance

ISS—Integrated Sensor System

ISSL—Initial Spares Support List

ISSM—Information System Security Manager

ISSO—Information System Security Officer

IST—Inter-Switch Trunk

ISvs—Information Service

IT—Information Technology

ITM—Information Technology Management

ITMRA—Information Technology Management Reform Act of 1996

ITN—Information Transfer Node

IT/NSSRD—Information Technology/National Security Systems Requirements Document

ITOS—Interim Tactical Orderwire System

ITS—1. Information Transfer System
2. Information Technology System(s)

ITSEC—Information Technology Security

ITU—International Telecommunications Union

IV&V—Independent Verification and Validation

IVD—1. Interactive Video Disk
2. Interactive Video Display

IVOS—Interior Voice Communications System

IVSN—Initial Voice Switched Network

IW—Information Warfare

IWS—Information Warfare Squadron

JATS—Jamming Analysis Transmission Selection

JBS—Joint Broadcast Services

JCCC—1. Joint Combat Camera Center
2. Joint Communications Control Center

JCEOI—Joint Communications-Electronics Operating Instruction

JCN—Joint Communications Network

JCSC—1. Joint Communications Satellite Center
2. Joint Communications Support Command

JCSE—Joint Communications Support Element

JDD—Job Data Documentation

JETDS—Joint Electronic Type Designation System

JFMO—Joint Frequency Management Office

JITC—Joint Interoperability Test Center

JMAPS—Joint Message Analysis and Processing System

JMAS—Joint Mission Application Software

JPEG—Joint Photographic Experts Group

JR—Jam Resistant

JRFL—Joint Restricted Frequency List

JRSC—Jam-Resistant Secure Communications

JRSC/SCP—Jam-Resistant Secure Communication/Secure Conferencing Project

JSIR—Joint Spectrum Interference Resolution

JSP—Joint SATCOM Panel

JTA—Joint Technical Architecture

JTIDS—Joint Tactical Information Distribution System

JTP—Joint Test Publication

JUDI—Joint Universal Data Interpreter

JWID—Joint Warfare Interoperability Demonstration

K—Kilo (thousand)

Kb—Kilobit

KAK—Key-Auto-Key

KB—Kilobyte

kbps—Kilobits Per Second

KDC—Key Distribution Center

KEK—Key Encryption Key

KG—Key Generator

kHz—Kilohertz

KMC—Key Management Center

KMID—Key Management Identification Number

KMODC—Key Management Ordering and Distribution center

KMP—Key Management Protocol

KMS—Key Management System

KMSA—Key Management System Agent

KMUA—Key Management User Agent

KP—Key Processor

KPK—Key Production Key

KPP—Key Performance Parameters

KSD—Key Storage Device

KSOS—Kernelized Secure Operating System

kt—Knot(s) (nautical mile per hour)

KTS—Key Telephone System

kVA—Kilovoltampere

KVD—Keyboard Visual Display

KVDT—Keyboard Video Display Terminal

KVDU—Keyboard Video Display Unit

KVG—Key Variable Generator

KVG—Key Variable Generator

kW—Kilowatt

L—Limited Distribution

LAA—Large Aperture Antenna

LAN—Local Area Network

LANT—Atlantic Ocean (area footprint)

LAN-OS—LAN Operating Systems

LAP—Link Access Procedure

LAP-B—Link Access Protocol - Balanced

LAP-D—Link Access Protocol - D channel

LAT—Latitude

LATA—Local Area Telecommunications Architecture

LAU—Line Amplifier Unit

LBB—Lower Beam Blanking

LBD—Laser Beam Detector

LBT1—Limited Bandwidth T1

LC—Liquid Crystal

LCATS—Large Capacity Automated Telecommunications System

LCC—Life Cycle Cost

LCD—Liquid Crystal Display

LCSP—Local Call Service Position

LD—Laser Diode

LDAP—Lightweight Directory Access Protocol

LDC—Local Display Console

LDDI—Local Distributed Data Interface

LDM—1. Limited Distance Modem
2. Logical Data Model

LDMX—Local Digital Message Exchange

LDR—Low Data Rate

LEAD—Low-Cost Encryption/Authentication Device

LEAF—Law Enforcement Access Field

LEASAT—Leased Satellite Communications System

LEC—Local Exchange Carrier

LED—Light-Emitting Diode

LEO—Low Earth Orbit

LER—Label Edge Router

LF—Low Frequency

LHITA—Long Haul Information Transfer Architecture

LIDAR—Light Detection and Ranging

LIME—Laser Induced Microwave Emissions

LITA—Local Information Transfer Architecture

LITS—Local Information Transfer System

LKG—Loop Key Generator

LM—Laser Module

LMD—Local Management Device

LMD/KP—Local Management Device/Key Processor

LMDS—Local Multipoint Distribution Service

LME—Layer Management Entry

LMI—Layer Management Interface

LMR—Land Mobile Radio

LMST—Lightweight Multiband Satellite Terminal

LNA—Low Noise Amplifier

LNB—Low Noise Block

LNC—Low Noise Converter

LO—Local Oscillator

LOC—Line(s) of Code

LON—Longitude

LORAN—Long Range Radio Aid to Navigation

LOS—Line-of-Sight

LP—1. Laser Printer
2. Low Power

LPA—Low Power Amplifier

LPC—Linear Predictive Coding

LPD—Low Probability Of Detection

LPI—Low Probability Of Intercept

LPM—Lines Per Minute

LPU—1. Line Printer Unit
2. Link Processing Unit

LRA—Local Reproduction Authorized

LRIP—Limited Rate Initial Preproduction

LRM—Low Rate Multiplexer

LRMM—Limited Remote Maintenance Monitor

LRR—Long-Range Radar

LRU—Line Replaceable Unit

LSA—Logistics Support Analysis

LSAT—Light multi-band Satellite Terminal

LSB—1. Least Significant Bit
2. Lower Sideband

LSD—Least Significant Digit

LSDA—Local Directory System Agent

LSI—Large Scale Integration

LSN—Local Serial Number

LSR—Label Switch Router

LSTDM—Low Speed Time Division Multiplex

LSU—1. Line Switch Unit
2. Line Sharing Unit

LTC—Low Target Count

LTL—Listening Time Limit

LTU—Line Termination Unit

LUF—Lowest Useable Frequency

LWIR—Long Wavelength Infrared

LWIRJ—Long Wavelength Infrared Jammer

MAC—1. Media Access Control
2. Message Authentication Code

m—Meter(s)

M&S—Modeling and Simulation

M-hop—Multiple hop

MAC—Media Access Control

MAGRAM—Magnetic Random Access Memory

MAIS—Major Automated Information System

MAN—Metropolitan Area Network

MAO—Mail Address Only

MARS—Military Affiliated Radio System

MART—Modular Automated Remote Terminal

MAST—MILSTAR Advanced Satellite Terminal

MathML—Mathematical Markup Language

Mb—Megabit

MB—Megabyte

MBA—Multi-Beam Antenna

MBd—Megabaud

MBMMR—Multi-Band Multi-Mode Radio

Mbps—Megabits per second

MC—Mission Capable

MCA—1. Mail Control Activity
2. Multichip Assembly

MCCB—Modification Configuration Control Board

MCCR—Mission Critical Computer Resources

MCE—Modular Control Equipment

MCEB—Military Communications-Electronics Board

MCF—Maintenance Control Facility

MCLDR—Matrix Controller Line Driver

MCM—Multichip Module

MCPU—Maintenance Control Processor Unit

MCU—Multifunction Control Unit

MCS—Message Conversion System

MDB—Main Data Bus

MDC—1. Manipulation Detection Code
2. Message Distribution Center

MDF—Main Distribution Frame

MDR—Medium Data Rate

MDS—Minimum Discernible Signal

MDT—1. Message Distribution Terminal
2. Mean Down Time

MDU—Maintenance Display Unit

MECL—Minimum Essential Circuit Listing

MEECN—Minimum Essential Emergency Communications Network

MEMS—Micro-Electro-Mechanical System

MEO—Medium Earth Orbit

MER—Minimum Essential Requirements

MF—Medium Frequency

MFD—Multifunction Display

MFI—Monitoring and Fault Isolation

MH—Message Host

MHF—Medium High Frequency

MHS—Message Handling System

MHz—Megahertz

MI—Message Indicator

MIB—Management Information Base

MICK—Mobility Initial Communications Kit

MIDAS—Military/International Dispatch and Accounting System

MIF—Multiple Interface

MIJI—Meaconing, Interference, Jamming, and Intrusion

MIL-HDBK—Military Handbook

MILNET—Military Network

MILO—Magnetically Insulated Line Oscillator

MILSAT—Military Satellite

MILSATCOM—Military Satellite Communications

MILSTAR—Military Strategic and Tactical Relay System

MIL-STD—Military Standard

MIMIC—Microwave/Millimeter wave Monolithic Integrated Circuit

MINSL—Minimum Security Level

MINTERM—Miniaturized Terminal

MIPR—Military Interservice Procurement Request

MIPS—Millions of Instructions Per Second

MIRA—Microprocessor Integrated Reliable Architecture

MISSI—Multilevel Information System Security Initiative

MKS—Meter-Kilogram-Second

MLB—Main Lobe Blanking

MLP—Multi-Line Phone

MLPP—Multilevel Precedence and Preemption

MLS—1. Microwave Landing System
2. Multi-Level Security

MMC—Modular Mission Computer

MMI—Man-Machine Interface

MMIC—Microwave Monolithis Integrated Circuit

MMLS—Mobile Microwave Landing System

MMRT—Modified Miniaturized Receive Terminal

MMT—Multimedia Terminal

MNCS—Master Net Control Station

MOD—Military Affiliate Radio System (MARS) Operating Directive

MODEM—Modulator/Demodulator

MODIS—Military Origin/Destination Information System

MOS—Monolithic Oxide Silicon

MPC—Multimedia Personal Computer

MPD—Master Power Distributor
Message Preparation Directory

MPDT—Message Processing Data Terminal

MPEG—Moving Picture Experts Group

MPI—Message passing Interface

MPL—1. Multischedule Private Line

2. Master Publication Library

MPLS—Multi-Protocol Label Switching

MPM—Microwave Power Module

MPOE—Minimum Point of Entry

MPU—Message Processing Unit

MRA—Minimum Receive Antenna

MRAM—Magnetoresistive Random Access Memory

MRK—Manual Remote Keying

MRT—1. Miniaturized Receive Terminal
2. Mean Repair Time

MS—1. Message Switch
2. Mail Service

MSB—Most Significant Bit

MSD—Most Significant Digit

msec—Millisecond

MSE—Mobile Subscriber Equipment

MSF—Multiplex Signal Format

MSL—Master Station Log

MSRT—Mobile Subscriber Radiotelephone Terminal

MSRV—Message Switch Rekeying Variable

MSS—Mobile Satellite Service(s)

MSU—Main Storage Unit

MSW—Mission Software

MTA—Message Transfer Agent

MTBCF—Mean Time Between Critical Failures

MTBF—Mean Time Between Failures

MTBM—Mean Time Between Maintenance

MTBOMF—Meant Time Between Operational Mission Failures

MTC—Magnetic Tape Controller

MTF—1. Message Text Formatting
2. Modulation Transfer Function

MTG—Master Timing Generator

MTI—Moving Target Indicator

MTTR—Mean Time To Repair

MTTRF—Mean Time to Restore Functions

MUF—Maximum Useable Frequency

MUI—Management User Interface

MUOS—Mobile User Objective System

MUX—Multiplex(er)

MVS—Multiple Virtual Storage

MW—1. Megawatt
2. Microwave

n—Nano

NA—Network Administration

NAAS—North American Air Surveillance

NAC—National Agency Check

NACAM—National COMSEC Advisory Memorandum

NACSI—National COMSEC Instruction

NACSIM—National COMSEC Information Memorandum

NADIN—National Airspace Digital Information Network

NAK—Negative Acknowledge

NARA—National Archives and Records Administration

NAS—1. Network Attached Storage
2. National Airspace System

NAT—Network Address Translator

NB—Narrowband

NBST—Narrowband Secure Terminal

NCC—Network Control Center

NCS—1. National Communications System
2. National Cryptologic School
3. Network Control Station
4. Node Center Switch

NCSC—National Computer Security Center

NCIT—Non-Coherent Integration Time

NCNR—Normalized Clutter-to-Noise Ratio

NDB—Non-Directional Beacon

NDE—Non-Destructive Evaluation

NDI—Non-Developmental Item

NDIS—Network Driver Interface Specification

NDS—1. Network Directory Service
2. Non-Developmental Software

NES—Network Encryption Standard

NETS—Nationwide Emergency Telecommunications System

NEXRAD—Next Generation Radar

NF—Noise Figure

NFE—Network Front End

NFS—Network File System

NGCR—Next Generation Computer Resources

NIB—Non-Interference Basis

NIC—1. Network Information Center
2. Network Interface Card

NID—Network-Inward Dialing

NIDMO—Network-Inward Dialing, Manual Out

NII—National Information Infrastructure

NIPRNET—Non-Secure Internet Protocol Router Network

NIS—Network Information Services

NISAC—National Industrial Security Advisory Committee

N-ISDN—Narrowband Integrated Switched Digital Network

NIST—National Institute of Standards and Technology

NLO—Non-Linear Optics

NMC—Not Mission Capable

nmi—Nautical Mile(s)

NNTP—Network News Transfer Protocol

NOC—1. Not Otherwise Coded
2. Network Operations Console

NOD—Network Outward Dialing

NOS—Network Operating System

NOSC—Network Operations and Security Center

NRTS—Not Repairable This Station

NRZ—Non Return to Zero

NSA—National Security Agency

NSAD—Network Security Architecture and Design

NSD—National Security Directive

NSDD—National Security Decision Directive

NSEP—National Security Emergency Preparedness

NS—Non-Secure

NSI—National Security Information

NSM—Network Security Monitor

NSO—Network Security Officer

NSP—Network Service Protocol

NSS—National Security System(s)

NSTAC—National Security Telecommunications Advisory Committee

NSWT—Non-Secure Warning Tone

NT—Net Terminal

NTC—Network Terminal Concentrator

NTCB—Network Trusted Computing Base

NTIA—National Telecommunications and Information Administration

NTIS—National Technical Information Service

NTISSAM—National Telecommunications and Information Systems Security Advisory/Information Memorandum

NTISSI—National Telecommunications and Information Systems Security Instruction

NTISSP—National Telecommunications and Information Systems Service Policy

NTIU—Network Terminal Interface Unit

NTP—Network Time Protocol

NVM—Nonvolatile Memory

NVRAM—Nonvolatile Ram

NVT—Network Virtual Terminal

O/PTN—Operationalize and Professionalize the Network

OA—Office Automation

OADR—Originating Agency's Determination Required

OC—Optical Carrier

OCA—Original Classification Authority

OCD—Operational Coverage Diagram

OCI—Offensive Counterinformation

OCR—Optical Character Reader

ODBC—Open Data Base Compliant

ODI—Open Datalink Interface

ODIS—Origin/Destination Information System

ODT—Optical Digital Technologies

OEM—Original Equipment Manufacturer

OF—Optional Form

OHCI—Open Host Controller Interface

OL—Operating Location

OLDR—Off-Line Data Reduction

OLS—On-Line Surveys

OLTP—On-Line Transaction Processor

OMC—Official Mail Center

OMR—Optical Mark Reader

ONA—Open Network Architecture

ONC—Open Network Computing

OOD—Object Oriented Design

OOS—Out-of-Service

OPCODE—Operations Code

OPCON—Operational Control

OPLAN—Operations Plan

OPSEC—Operations Security

OPTN—Optimizing The Network

OPX—Off Premise Extension

OQPSK—Octagonal Quadrature Phase Shift Keying

ORA—Organizational Registration Authority

ORD—Operational Requirements Document

OS—Operating System

OSA—Open System Architecture

OSE—Open System Environment

OSF—Open Software Foundation

OSI—Open Systems Interconnection

OSPF—Open Shortest Path First

OSW—Operational Software

OT&E—Operational Test and Evaluation

OTAD—Over-The-Air key Distribution

OTAR—Over-The-Air Rekey

OTAT—Over-The-Air key Transfer

OTDR—Optical Time Domain Reflectometer

OTH—Over-the-Horizon

OTI—Office of Technical Integration

OTP—One-Time Pad

OTS—Off-the-Shelf

OTSS—Operational Telecommunications Switching System

OTT—One-Time Tape

OW—Order Wire

P—1. Priority
2. Power (Watts)

Pavg—Power, Average

Ppk—Power, Peak

PA—1. Privacy Act
2. Power Amplifier
3. Product Announcement

PAA—Policy Approving Authority

PAAP—Peer Access Approval

PABX—Private Automatic Branch Exchange

PAC—Pacific Ocean (area footprint)

PACE—Performance Analysis by Continuous Evaluation

PAD—1. Packet Assembler/Disassembler
2. Power Attenuation Device

PAL—1. Program Assembler Language
2. Parcel Airlift
3. Phase Alternate Line

PAP—Password Authentication Protocol

PAS—Privacy Act Statement

PAX—Private Automatic Exchange

PB—1. Postal Bulletin
2. Publishing Bulletin

PBX—Private Branch Exchange

PC—1. Personal Computer 2. Photoconductive

PC/NFS—Personal Computer/Network File System

PCA—Physical Configuration Audit

PCB—Printed Circuit Board

PCI—Peripheral Component Interface

PCM—Pulse-Code Modulation

PCMCIA—Personal Computer Memory Card International Association

PCMT—Personal Computer Message Terminal

PCS—Personal Communications System

PCU—Power Converter Unit

PCZ—Protected Communications Zone

PD—1. Pulse Duration
2. Probability of Detection
3. Policy Dorective

PDA—Personal Digital Assistant

PDC—1. Program Designator Code
2. Primary Domain Controller

PDF—Precision Direction Finder

PDH—Plesiochronous Digital Hierarchy

PDI—1. Picture Description Language
2. Power Data Interface

PDL—Publication Distribution Library

PDM—Publishing Distribution Manager

PDP—1. Procedure Definition Processor
2. Programmed Data Processor

PDR—Preliminary Design Review

PDS—1. Protected Distribution System
2. Practice Dangerous to Security

PDU—1. Power Distribution Unit
2. Protocol Data Unit

PE—Phase Encoded

PEP—Peak Envelope Power

PES—Positive Enable System

PFM—Pulse Frequency Modulation

PGWS—Primary Groupware Server

PHz—Petahertz

PIA—Peripheral Interface Adapter

PIC—Plastic Insulated Cable

PIF—Productivity Investment Fund

PIM—1. Procedural Instruction Message
2. Processor in Memory

PIN—Personal Identification Number

PING—Packet INternet Groper

PITN—Primary Information Transfer Nodes

PK—Public Key

PKA—Public Key Algorithm

PKC—Public Key Cryptography

PKI—Public Key Infrastructure

PKSD—Programmable Key Storage Device

PLA—Plain Language Address

PLD—Programmable Logic Device

PLL—Phase Locked Loop

PLN—Private Line Network

PLO—Phased Locked Oscillator

PLP—1. Packet Layer Protocol
2. Procedural Language Processor

PM—Phase Modulation

PMD—Program Management Directive

PMI—Preventive Maintenance Inspection

PMFI—Performance Monitoring and Fault Isolation

PnP—Plug-and-Play

POP—1. Post Office Protocol
2. Point Of Presence

POSE—Picture Oriented Software Engineering

POSI—Portable Operating System Interface

POSIX—Portable Operating System Interface for Computer Environments

POTS—Purchase of Telecommunication Service

PPI—Plan Position Indicator

PPL—Preferred Products List (a section in the *Information Systems Security Products and Services Catalogue*)

PPM—1. Pages Per Minute
2. Pulse Position Modulation

PPP—Point-to-Point Protocol

PPS—1. Packets Per Second
2. Pulse Per Second

PRI—Pulse Recurrence Interval

PRF—Pulse Recurrence Frequency

PRISM—Programmable-Reconfigurable-Integrated-Switch and Multiplex

PRODSEC—Product Security

PROM—Programmable Read-Only Memory

PROPIN—Proprietary Information

PRR—Pulse Repetition Rate

PRT—Pulse Repetition Time

PSCF—Primary System Control Facility

PSL—Protected Services List

PSN—Packet Switching Node

PSS/CCTV—Perimeter Surveillance System/Closed Circuit Television

PSTN—1. Packet Switched Telecommunications Network
2. Public Switched Telephone Network

PT—Printer-only Terminal

PTF—Patch and Test Facility

PTM—Packet Transfer Mode

PTP—Point-to-Point

PTSN—Public Telephone Switching Network

PTT—Push-to-Talk

PVC—Permanent Virtual Circuit

PW—Pulse Width

PWCS—Personal Wireless Communications System

PWDS—Protected Wireline Distribution System

QA—Quality Assurance

QAE—Quality Assurance Evaluator

QAM—Quadrature Amplitude Modulator

QC—Quality Control

QFIRC—Quick Fix Interference Reduction Capability

QoS—Quality of Service

QPSK—Quadrature Phase Shift Keying

QRC—Quick Reaction Capability

QRCT—Quick Reaction Capability Terminal

QRP—1. Query and Reporting Processor
2. Quick Reaction Package

QRSA—Quick Reaction Satellite Antenna

QSP—Quick System Profile

QTP—Qualification Training Package

R—Routine

R/T—Receive/Transmit

RACE—Rapid Automatic Cryptographic Equipment

RADAR—Radio Detection and Ranging

RADAY—Radio Day

RADEX—Radar Data Extractor

RADHAZ—Radiation Hazard

RAG—Range Azimuth Gate

RAM—Random Access Memory

RAPPI—Random Access Plan Position Indicator

RARP—Reverse Address Resolution Protocol

RAS—Remote Access Service

RAU—Radio Access Unit

RBD—Radar Beacon Digitizer

RC—1. Resistive-Capacitive
2. Records Custodian

RCC—Regional Control Center

RCI—Radar Coverage Indicator

RCS—1. Report Control Symbol
2. Radar Cross Section

RCU—Remote Control Unit

RCVR—Receiver

RDB—Relational Data Base

RDD—Required Delivery Date

RDI—Radar Data Interface

RDL—Remote Data Link

RDM—Relational Data Base Machine

RDMS—Relational Data Base Management System

RDPC—Regional Data Processing Center

RDS—Records Disposition Schedule

RDT—Remote Digital Terminal

RDU—Radar Display Unit

REM—Recognition Memory

RF—Radio Frequency

RFA—Radio Frequency Authorization

RFCM—Radio Frequency Countermeasure

RFCMOS—Radio Frequency Complimentary Metal-Oxide Semiconductor

RFE—Receiver Front End

RFI—Radio Frequency Interference

RFM—Radio Frequency Module

RFO—Radio Frequency Oscillator

RFS—1. Remote File System
2. Request for Service

RGB—Red/Green/Blue

RGPD—Range Gated Pulse Doppler

RHI—Range Height Indicator

RI—Routing Indicator

RICK—Rapid Initial Communications Kit

RIMS—Records Information Management System

RIP—Routing Information Protocol

RLP—Remote Line Printer

RMS—1. Reliability, Maintainability, Supportability
2. Remote Monitoring Subsystem

RN—Relay Node

RNP—1. Remote Network Printer
2. Remote Network Processor

RNR—Receive Not Ready

RO—Receive Only

ROA—Remote Optical Assembly

ROD—Required Operational Date

ROM—Read-Only Memory

ROP—Receive-Only Printer

ROSC—Regional Operations and Security Center

ROW—Return Orderwire

RP—1. Recurring Periodical
2. Restoration Priority

RPC—1. Regional Processing Center
2. Remote Processing Computer

RPL—Restoration Priority List

RPPO—Regional Printing Procurement Office

RQT—Reliability Qualification Tests

RR—Radio Regulations of the International Telecommunications Union

RSBC—Routing Signalling Buffer Controller

RSI—1. Remote Symbiotic Interface
2. Remote Status Indicator

RSLS—Receiver Side Lobe Suppression

RSN—RED Switch Network

RSS—Routing Subsystem

RSSC—Regional SATCOM Support Center

RST—Remote Switching Terminal

RSU—Remote Switching Unit

RSVP—ReSerVation setup Protocol

RTCP—Real-Time Communications Protocol

RTE—Remote Terminal Emulator

RTL—Radar Threshold Limit

RTOS—Real-Time Operating System

RW—Read/Write

RWR—Radar Warning Receiver

RX—Receive

RZ—Return-to-Zero

S&I—Stock and Issue

S&T—Science and Technology

S/N—Signal-to-Noise Ratio

S/V—Survivability/Vulnerability

SA—1. Security Assistance
2. System Administrator

SAA—1. Satellite Access Approval
2. Small Aperture Antenna

SAC—Semi-Automatic Controller

SADL—Situational Awareness Data Link

SALTS—Standard Automated Logistics Tool Set

SAM—Space Available Mail

SAMM—Security Assistance Management Manual

SAN—1. System Advisory Notice
2. System Area Network
3. Storage Area Network

SAO—Special Access Office

SAP—Special Access Program

SAR—1. Subaccount Representative
2. Service Activation Request
3. Satellite Access Request
4. Synthetic Aperture Radar
5. Special Access Required

SARSAT—Search and Rescue Satellite-Aided Tracking

SAS—Single Audio System

SAT—1. Satellite
2. Systems Acceptance Test

SATCOM—Satellite Communications

SBIT—Standard Base Infrastructure Template

SBL—Space-Based Laser

SBLC—Standard Base-Level Computer

SBLCC—Standard Base-Level Communications-Computer

SBSS—Standard Base Supply System

SBU—Sensitive But Unclassified

SCAMP—Single Channel Anti-jam Man-Portable (terminal)

SCCB—Software Configuration Control Board

SCCC—Satellite Communications Control Center

SCCE—Satellite Configuration Control Element

SCDL—Surveillance and Control Data Link

SCI—1. Sensitive Compartmented Information
2. System Control Interface

SCINET—Sensitive Compartmented Information Network

SCIS—Survivable Communications Integration System

SCM—Scramble Code Multiplexer

SCN—1. Satellite Communications Node
2. System Change Notice

SCOC—Systems Control and Operations Concept

SCOTT—Single Channel Objective Tactical Terminal

SCR—Signal-to-Clutter Ratio

SCS—Silicon Controlled Switch

SCSC—Small Computer Support Center

SCSI—Small Computer System Interface

SCT—1. Satellite Communications Terminal
2. Single Channel Transponder
3. Secure Cellular Telephone

SCTC—Small Computer Technical Center

SCTS—Single Channel Transponder System

SCV—Subclutter Visibility

SDA—Software Design Activity

SDC—Signal Data Converter

SDE—Source Data Entry

SDH—Synchronous Digital Hierarchy

SDIF—SGML Document Interchange Format

SDL—Software Development Library

SDMA—Space Division Multiple Access

SDMX—Space Division Matrix

SDN—System Development Notification

SDNRIU—Secure Digital Net Radio Interface Unit

SDNS—Secure Data Network System

SDP—1. Software Development Plan
2. Service Delivery Point

SDS—Space Defense System

SDSL—Symmetric Digital Subscriber Line

SDT—Software Development Tool

SE—1. Software Engineering
2. Software Evaluator

SEN—Small Extension Node

SEON—Solar Electro-Optical Network

SERL—System Engineering Reference Library

SETA—System Engineering and Technical Assistance

SF—Standard Form (*used on designated forms*)

SFA—Security Fault Analysis

SFAF—Standard Frequency Action Format

SFS—Shared File System

SFUG—Security Features Users Guide

SGDB—Satellite Global Data Base

SGML—Standard Generalized Markup Language

SGRAM—Synchronous Graphics Ransom Access Memory

SHA—Secure Hash Algorithm

SHD—Special Handling Designator

SHF—Super High Frequency

SHTTP—Secure Hypertext Transfer Protocol

SI—Special Intelligence

SIB—System Interface Bus

SIDS—1. Satellite Information Dissemination System
2. Secondary Imagery Dissemination System

SIGINT—Signals Intelligence

SIGSEC—Signals Security

SII—System Internal Interface

SIM—SATCOM Interface Module

SIMM—Single In-line Memory Module

SINCGARS—Single Channel Ground and Airborne Radio System

SIP—1. Serial Interface Port
2. Session Initiation Protocol

SIPRNET—Secret Internet Protocol (IP) Router Network

SIPTO—Standard Installation Practice Technical Order

SITN—Secondary Information Transfer Nodes

SIU—Storage Interface Unit

SL—Sensitivity Level

SLA—Service Level Agreement

SLB—Side Lobe Blanker

SLC—Subscriber Line Concentrator

SLFCS—Survivable Low Frequency Communications System

SLIP—Serial Line Internet Protocol

SLL—Side Lobe Level

SLOC—Source Line of Code

SLP—Single Line Phone

SLS—Side Lobe Suppression

SMART—Self-Monitoring Analysis And Reporting Technology

SMART-T—Secure Mobile Anti-jam Reliable Tactical - Terminal

SMDS—Switched Multimegabit Data Service

SMI—Security Management Infrastructure

SMN—Secure Multi-Networking

SMP—Symmetric Multiprocessing

SMR—Specialized Mobile Radio

SMSC—Standard Multi-User Small Computer

SMSCRC—Standard Multi-User Small Computer Requirements Contract

SMT—1. Surface Mail Transport
2. Special Maintenance Team

SMTP—1. Simple Mail Transfer Protocol

2. Simple Message Transfer Protocol

SMU—Secure Mobile Unit

SN—Serial Number

SNA—Systems Network Architecture

SNI—1. Standard Network Interface
2. Subscribers Network Interfaces
3. System Network Interconnect

SNMP—Simple Network Management Protocol

SNR—Signal-to-Noise Ratio

SNRAT—Signal-to-Noise vs. Range, Altitude, and Tilt

SOAP—Simple Object Access Protocol

SOCR—Stand-Alone Optical Character Reader

SOCS—Strategic Operations Communications System

SON—Statement of Need

SONET—Synchronous Optical Network

SOQPSK—Shaped Offset Quadrature Phase Shift Keying

SP—Security Preferred

SPA—Software Process Assessment

SPECAT—Special Category

SPI—1. Security Profile Inspector
2. System Programming Interface

SPIN—Software Process Improvement Network

SPIP—Software Process Improvement Program

SPK—Single Point Key(ing)

SPN—Shared Processing Network

SPS—Scratch Pad Store

SQL—Structured Query Language

SRA—Sub-Registration Authority

SRAM—Static Random Access Memory

SRD—1. Standard Reporting Designator
2. Systems Requirement Document

SRIP—Software Reuse Implementation Plan

SRR—Security Requirements Review

SSA—1. Software Support Activity

2. Solid State Amplifier

SSB—Single Sideband

SSI—Signal-Strength Indicator

SSMA—Spread-Spectrum Multiple Access

SSO—Special Security Officer

SSP—System Support Processor

SSR—1. Solid State Receiver
2. Secondary Search Radar

SSUPS—Solid State Uninterruptible Power Supply

ST—Subscriber Terminal

ST&E—Security Test and Evaluation

STALO—Stable Local Oscillator

STAMPS—Stand-Alone Message Processing System

STANAG—Standardization Agreement

STAR—System Threat Assessment Report

STATMUX—Statistical Multiplexer

STC—Sensitivity Time Control

STDM—Synchronous Time Division Multiplexing

STE—Secure Terminal Equipment

STEM—Systems Telecommunications Engineering Manager

STEM-B—Systems Telecommunications Engineering Manager-Base Level

STEM-C—Systems Telecommunications Engineering Manager-Command Level

STEM-J—Systems Telecommunications Engineering Manager-Joint

STEM-R—Systems Telecommunications Engineering Manager-ANG Regional

STEM-TM—Systems Telecommunications Engineering Manager-Technical Manager

STEP—Standardized Tactical Entry Point

STFS—Standard Time and Frequency Signal (Service)

STID—Standard Identification

STINFO—Science and Technology Information

STM—Synchronous Transfer Mode

STP—Shielded Twisted Pair

STRAP—Surveillance and Tracking Radar Processor

STS—1. Subcommittee on Telecommunications Security

2. Synchronous Transport Signal

STT—Satellite Tactical Terminal

STU-III—Secure Telephone Unit III

STV—Surveillance Television

SUM—Software User's Manual

SVC—Switched Virtual Circuit

SVGA—Super Video Graphics Array

SVM—Secure Voice Module

SVS—Switched Voice Service

SW—Software

SWR—Standing Wave Ratio

SYS—System

SYSCON—System(s) Control

SYSGEN—System Generation

T—(Noise) Temperature

T&E—Test and Evaluation

T&S—Timing and Synchronization

TA—1. Technical Architecture
2. Traffic Analysis

TAA—Transmit Antenna Array

TAC—1. Terminal Access Controller
2. Tactical

TACAN—Tactical Air Navigation

TACSAT—Tactical Satellite

TACTED—Tactical Trunk Encryption Device

TACTERM—Tactical Terminal

TADIL—Tactical Digital Information Link

TADIL-J—Tactical Digital Information Link - Joint

TADIX—Tactical Digital Information Exchange

TAG—1. Tempest Advisory Group
2. Transmit Antenna Groundscreen

TAISS—Telecommunications and Automated Information System Security

TAR—Telecommunications Assessment Report

TB—TeraBytes

TBA—Terminal Base Address

TBF—Transmit beam Former

TBMCS—Theater Battle Management Core System

TBVC—Terminal Box, Video Cable

TCA—Tactical Communications Architecture

TCB—Trusted Computing Base

TCC—Telecommunications Center

TCCF—Tactical Communications Control Facility

TCD—Time Compliance Data

TCF—Technical Control Facility

TCM—Time Compression Multiplexing

TCMD—Transportation Control and Movement Document

TCO—1. Telecommunications Certification Office/Officer
2. Telecommunications Control Office
3. Telephone Control Officer

TCOM—Tethered Communications

TCP—Transmission Control Protocol

TCP/IP—Transmission Control Protocol/Internet Protocol

TCSEC—Trusted Computer System Evaluation Criteria

TCSS—Telecommunications Systems Standard

TD—Transfer Device

TDC—Theater Deployable Communications

TDF—Tactical Digital Facsimile

TDL—Tactical Data Link

TDM—Time Division Multiplexer

TDMA—Time Division Multiple Access

TDMF—Time Division Matrix Function

TDMM—Time Division Memory Module

TDMX—Time Division Matrix

TDP—Technical Data Package

TDR—Time Domain Reflectometer

TE—Test Equipment

TED—Trunk Encryption Device

TEK—Traffic Encryption Key

TELEFAX—Telecommunications Facsimile

TELNET—Telecommunications Network

TEP—Tempest Endorsement Program

TeraOps—Trillion Operations Per Second

TFIB—Tag Forwarding Information Base

TFM—Trusted Facility Manual

TFS—1. Time Frequency Standard
2. Traffic Flow Security

TFTP—Trivial File Transfer Protocol

THF—Tremendously High Frequency

THSDN—Tactical High Speed Data Network

THz—Terahertz

TIA—Transmission Interface Adapter

TID—Touch Interactive Display

TIFF—Tag Image File Format

TIP—Terminal Interface Processor

TIR—Technical Integration Repository

TITN—Tertiary Information Transfer Nodes

TLMR—Trunked Land Mobile Radio

TLS—1. Top-Level Specification
2. Transport Layer Security

TM—1. Technical Manual
2. Telemetry

TMAP—Telecommunications Monitoring and Assessment Program

TMDE—Test, Measurement, and Diagnostic Equipment

TMET—Transportable Medium Earth Terminal

TMR—Telecommunications Monitoring Report

TMS—Telecommunications Management System

TMSC—Transportation Management Service Center

TMUX—Terminal Multiplexer

TNI—Trusted Network Interpretation

TNIEG—Trusted Network Interpretation Environment Guideline

TO—Technical Order

TOF—Time of File

TOR—Time of Receipt

TOT—Time of Transmission

TP—Transaction Processor

TPC—Two-Person Control

TPDL—Tempest Profile Data List

TPI—Two-Person Integrity

T/R—Transmit/Receive

TRANSEC—Transmission Security

TRC—Technical Reference Code

TREE—Transient Radiation Effects on Electronics

TRI-TAC—Tri-Service Tactical Communications

TRM—Technical Reference Model

TROPO—Tropospheric Scatter

TRS—Tracking and Reporting Software

TS—Top Secret

TSB—Trunk Signalling Buffer

TSCM—Technical Surveillance Countermeasures

TSD—Trunk Signalling Device

TSEC—Telecommunications Security

TSK—Transmission Security Key

TSO—Telecommunications Service Order

TSP—1. Telecommunications Service Priority
2. Time Synchronization Protocol

TSR—1. Telecommunications Service Request
2. Tag Switch Router

TSSP—Tactical Satellite Signal Processor

TSSR—Tropo Satellite Support Radio

TTA—Tactical Terminal Adapter

TT&C—Telemetry, Tracking, and Command

TTISSMM—Transit Time Information Standard System for Military Mail

TU—Timing Unit

TWR—Tactical Weather Radar

TWT—Traveling Wave Tube

TWTA—Traveling Wave Tube Amplifier

TX—Transmit

U/C—Upconverter

UA—User Agent

UAS—User Application Software

UCI—User Computer Interface

UDC—1. Unit Descriptor Code
2. Universal Downconverter

UDS—Universal Data System

UDP—User Datagram Protocol

UDT—Unstructured Data Transfer

UEF—User Exchange Format

UFO—UHF Follow-On

UFO/E—UHF Follow-On/EHF

UFO/EE—UHF Follow-On/Enhanced EHF

UHF—Ultra High Frequency

UHR—Ultra High Resolution (Radar)

UI—User Interface

UIC—Unit Identification Code

UIDL—User Interface Definition Language

UIL—User Interface Language

UIRK—Unique Interswitch Rekeying Key

UIS—User Interface System

UKB—Universal Keyboard

U/L—Uplink

ULANA—Unified Local Area Network Architecture

ULCS—Unit Level Circuit Switch

ULF—Ultra Low Frequency

UM—Universal Modem

UMB—Upper Memory Block

UMS—Universal Modem System

UPP—User Partnership Program

UPS—Uninterruptible Power Supply

UPT—Universal Personal Telecommunications

UR—Utilization Rate

URDB—User Requirements Data Base

URL—Uniform Resource Locator

URN—Uniform Resource Name

USB—1. Universal Serial Bus
2. Upper Sideband

U.S.C.—United States Code

USDE—Undesired Signal Data Emanations

USER-ID—User Identification

USHR—Unidirectional Self Healing Ring

USMTF—United States Message Text Formatting

USTS—UHF Satellite Terminal System

UT—1. Universal Time
2. User Terminal

UTP—Unshielded Twisted Pair

UTR—Uptime Ratio

UtRAM—Uni-transistor Random Access Memory

UTS—Universal Terminal System

UV—Ultraviolet

V—Volt(s)

VA—Volt-Ampere

VAC—Volts, Alternating Current

VAN—Value Added Network

VAPI—Virtual Application Programming Interface

VAX—Virtual Address Extension

VBR—Variable Bit Rate

VC—1. Virtual Channel
2. Voice Channel

VCI—Virtual Channel Identifier

VCO—Voltage Controlled Oscillator

VCSS—Voice Communications Switching System

VDC—Volts, Direct Current

VDI—Virtual Device Interface

VDM—Virtual Device Metafile

VDOC—Visual Documentation

VDS—Voice Data Switch

VDSL—Very high bit rate Digital Subscriber Line

VDT—Video Display Terminal

VDU—Visual Display Unit

VDUC—Visual Display Unit Controller

VF—Voice Frequency

VGA—Video Graphics Adapter

VHF—Very High Frequency

VHS—Video Handling System

VHSIC—Very High Speed Integrated Circuit

VIC—Vulnerability/Incident Control

VIP—1. Visual Information Processor
2. Variable Interpulse Period

VIR—Vulnerability and Incident Report

VIU—Video Interface Unit

VLAN—Virtual Local Area Network

VLF—Very Low Frequency

VLSI—Very Large Scale Integration

VME—Virtual Memory Expansion

VMF—Variable Message Format

VMM—Virtual Memory Manager

VMS—Virtual Memory System

VNMC—Video Network Management Center

VOCODER—Voice Coder Encoder-Decoder

VOCU—Voice Orderwire Control Unit

VoDSL—Voice over Digital Subscriber Line

VoIP—Voice over Internet Protocol

VOM—Volt-Ohmmeter

VOR—VHF Omni-directional Range

VORTAC—VHF Omni-Range Tactical Air Navigation

VOX—Voice actuation/actuated

VPI—Virtual Path Identifier

VPN—Virtual Private Network

VPO—Virtual Program Office

VRAM—Video Random Access Memory

VRML—Virtual Reality Modeling Language

Vrms—Volts, root-mean-square

VRS—Velocity Response Shape

VSAT—Very Small Aperture Terminal

VSS—1. Video Storage System
2. Voice Switching System

VST (CFD)—Vinson Subscriber Terminal (Common Fill Device)

VSWR—Voltage Standing Wave Ratio

VT—1. Virtual Terminal
2. Video Terminal

VTA—Video Terminal Adaptor

VTC—Video Teleconferencing

VTCN—Video Teleconference Communications Network

VTE—Video Teleconferencing Equipment

VTP—Virtual Terminal Protocol

VTT (CFD)—Vinson Trunk Terminal (Common Fill Device)

VTU—Video Teleconferencing Unit

VU—Volume Unit

W3C—World Wide Web Consortium

WADS—Wide Area Data Service

WAIS—Wide Area Information Service

WAN—Wide Area Network

WAP—Wireless Application Protocol

WARF—Wide Aperture Research Facility

WAS—Wide Area Surveillance

WATS—Wide Area Telecommunications Service

WBS—Wireless Broadband System

WBW—Waveform Bandwidth

WCCS—Wing Command and Control System

WDM—Wavelength Division Multiplexing

WEP—Wired Equivalent Privacy

WICP—Wing Initial Communications Package

WICS—Wing Integrated Communications System

WIN-T—Warfighter Information Network - Tactical

WLAN—Wireless Local Area Network

WMLS—Wireless Markup Language Specification

WOM—Write-Only Memory

WORM—Write-Once, Read-Many

WP—Word Processor

WPM—Words Per Minute

WRSK—War Readiness Spares Kit

WVDC—Working Voltage Direct Current

WWW—World Wide Web

X—Military Super High Frequency Band

XAP-TP—X/Open API-Transaction Processing

XCDR—X/Open CD-ROM

XDR—1. External Data Representation
2. Extended Data Rate

XDS—X/Open Directory Service

XLFD—X/Logical Font Description

XML—Extensible Markup Language

XMOG—X/Open Managed Object Guide

XMP—X/Open Management Protocol

XMPP—X/Open Management Protocol Profiles

XMS—Extended Memory Specification

XMTR—Transmitter

XNFS—X/Open Network File System

XNS—Extensible Name Service

XO—Crystall Oscillator

XT—Crosstalk

Z—ZULU Time

ZCS—Zero Code Suppression

ZIF—Zero Insertion Force

Zo—Charteristic Impedance

Terms

Acceptance (of a Communications and Information Facility/System)**—**Indicates a facility or system generally meets technical and performance standards but may have minor exceptions that do not keep the facility from meeting operational and security requirements.

Acceptance Inspection—The final inspection to determine if a facility or system meets the specified technical and performance standards. It is held immediately after facility and software testing, and is the basis for commissioning or accepting the C4 system.

Access—(1) A user's ability to communicate with (input to or receive output from) a system or to have entry to a specified area. (2) In satellite communications (SATCOM), the right to enter a SATCOM network and make use of the communications payload resources.

Access Control List (ACL)—Mechanism implementing discretionary and/or mandatory access control between subjects and objects.

Access Control Mechanism—Security safeguard designed to detect and deny unauthorized access and permit authorized access in an information system.

Access Lines—Two-wire or four-wire circuits that allow user equipment to gain access to a network.

Accessible Space—In information assurance, the area within which the user is aware of all persons entering and leaving. This area denies the opportunity for concealed TEMPEST surveillance, and delineates the closest point of potential TEMPEST intercept from a vehicle. Preferred term: Inspectable Space.

Access Switch—A generic term referring to a Defense Switched Network switch that serves users.

Accountability—In information assurance, the principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information.

Accounting Legend Code—In information assurance, a numeric code used to indicate the minimum accounting controls required for items of accountable COMSEC material within the COMSEC Material Control System.

Accreditation—Formal declaration by a designated approving authority (DAA) that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. The DAA provides written approval for the operation of each system or network before it can begin processing in a specified facility.

Accreditation Control Number (ACN)—Information concerning the status of a particular information system's accreditation that is entered into the Information Processing Management System (IPMS).

Accuracy—Free from error. Accuracy denotes the absolute quality of computed results. In contrast, precision refers to the degree to which computed results reflect theoretical values.

Acquisition—(1) In satellite communications, the process of locking tracking equipment on a signal from a communications satellite (referred to as "acquiring the satellite"). (2) The Department of Defense (DoD) process of conceptualization, initiation, design, development, testing, contracting, production, deployment, logistics support, modification, and disposal of weapons and other systems, supplies, or services (including construction) to satisfy DoD needs, intended for use in or in support of military missions.

Acquisition Program—A directed, funded effort designed to provide a new, improved, or continuing materiel, weapon, or information system or service capability in response to a validated operational or business need. Acquisition programs are divided into different categories that are established to facilitate decentralized decision-making, execution, and compliance with statutory requirements. Technology projects are not acquisition programs.

Adaptive Communications—A communications system, or part thereof, that automatically uses feedback information obtained from the system itself or from the signals carried by the system to modify dynamically one or more of the system operational parameters to improve system performance or to resist degradation.

Adaptive Radio—radio that (1) monitors its own performance, (2) monitors the path quality through sounding or polling, (3) varies operating parameters, such as frequency, power, or data rate, and (4) uses closed-loop action to optimize its performance by automatically selecting frequencies or channels.

Adjacent Channel—In a telecommunications system, the next channel or the one in close proximity, either physically or electrically, to the one in use.

Administrative Security—Management constraints and supplemental administrative controls established to provide an acceptable level of protection for data. Synonymous with Procedural Security.

Administrative Vulnerability—A information system's security weakness resulting from incorrect or inadequate security safeguards and controls attributable to the system administrator, Information System Security Officer, or user.

Adopted Form—A form that is listed in a publication other than its prescribing directive.

Advanced Research Projects Agency Network (ARPANet)—The precursor to the Internet. Developed in the late 1960's and early 1970's by the DoD as an experiment in wide-area networking that would survive a nuclear war.

Advocate—In system lifecycle management, a designated organization that represents the interests of a specific group of users of a communications system. The advocate does not directly speak for the users, but represents the users' interests at appropriate forums, such as requirements development, concept of operations development, specialized training, and operational assessments.

Aggregation—Collection or grouping of independent information where the sensitivity of the whole is greater than the sensitivity of the parts.

Air Force C4 Systems Architectures—A multi-volume family of documents that provides guidance on goals, objectives, and strategies for planning future C4 systems.

Air Force Electronic Publications Library (AFEPL)—The compact disk-read only memory based

repository of electronic publications and forms.

Air Force Engineering and Technical Services (AFETS)—Advisory, instructional, and technical training services provided by qualified civil service or contractor personnel in the installation, operation, and maintenance of weapon/communications systems and equipment used by Air Force organizations.

Air Force Equipment Management System (AFEMS)—The official inventory and account for communications, electronics, and other equipment centrally managed by Headquarters Air Force Materiel Command.

Air Force Information Architecture—A framework that depicts the relationships of elements involved in information management within an organization. Within the Air Force, it is used to provide a blueprint for developing specific plans and actions in the planning, control, and management of Air Force information.

Air Force Information Resources Dictionary System (AFIRDS)—A software tool used as a data dictionary for management of metadata (data about data). It supports research and maintenance of existing data elements and is used to create new elements using the DoD standardization guidelines.

Air Force Information Technology (IT) Infrastructure—The common set of core functions and resources that provide an environment of secure integrated communications, computing and information management capabilities, which enable multiple IT and National Security Systems (NSS), and support effective operations across the enterprise. It is comprised of five key components: (1) Communications Infrastructure (provides end-to-end connectivity), (2) Information Assurance Infrastructure (provides protection, detects intrusion/abnormal activity) and takes corrective actions, (3) Computing/Software Infrastructure (provides for common software/operating systems/environment), (4) Information Management Infrastructure (provides for overall management), and (5) Physical Infrastructure (all equipment, i.e., things, boxes, etc.). (AF CIO)

Air Force Integrated Telecommunications Network (AFNET)—A dedicated, high speed, wideband information transport system combining common user, and command, control, communications, and computer circuits into a single, integrated, centrally managed network. AFNET supports voice circuits and data circuits with rates from 1.2 kbps to 45 Mbps.

Air Force Portal—A world-class, integrated information tool that provides Air Force users secure, single log-on access to all information and mission applications required to execute their daily missions.

Air Force Satellite Communications (AFSATCOM)—System An ultra high frequency (UHF) satellite communications system that provides reliable UHF, two-way command and control communications between the National Command Authority and globally deployed nuclear forces. The system is composed of satellites of the United States Navy's Fleet Satellite Communications System, the Air Force's Satellite Data System, UHF single-channel transponders integrated into Defense Satellite Communications System III satellites, ground, and airborne terminals.

Air Technology Network—The standard Air Force video teletraining network. A satellite-based broadcasting system that includes uplink broadcasting facilities and downlink receiving sites at Air Force bases. The network provides one-way video and two-way audio communications.

Algorithm—A finite set of well-defined rules for the solution of a problem in a finite number of steps.

Algorithmic Language (ALGOL)—A high-level computer language used to express problem-solving formulas for machine solution.

Allied Long Lines Agency (ALLA)—A multinational organization organized under the North Atlantic Treaty Organization (NATO) to process and coordinate leased long-lines circuit orders of NATO, Supreme Headquarters Allied Powers Europe, and national military forces residing in the NATO area.

Allocated Circuit—A communications circuit designated for use (whether common user or dedicated).

Allocation—In satellite communications, the operational real-time assignment of communications payload resources to an approved user for use in activating a communications link or network.

Alternate Route (Altroute)—A secondary communications path used to reach a destination if the primary path is unavailable.

Alternate Use—An arrangement that permits the use of a circuit for different types of transmission such as voice, data, facsimile, magnetic tape, etc. Normally, only one type of operation is possible at any one time (alternate use), although simultaneous use is possible in some instances. The use of a circuit exclusively for voice communications, even though both secure and nonsecure voice conversations are passed over the circuit, is not considered alternate use.

Alternate Voice Data (AVD) or Alternate Voice Record (AVR)—Interchangeable terms that describe the alternate use of circuits when one use is for voice (non-record) conversations and the other use is for record communications. Transfer arrangements and conditioning equipment are normally required for alternate use. When a circuit is used exclusively for voice, even though the voice conversations may appear as data on the transmission path between the end terminals, the circuit is not considered as an alternate voice data or alternate voice record circuit.

Amendment—The process of adding, deleting, or changing information in a system of records to make the data accurate, relevant, timely, or complete.

American National Standard (ANS)—Any standard, supported by a national consensus, developed, approved, and cleared through the American National Standard Institute.

American National Standards Institute (ANSI)—The United States Standards organization that establishes procedures for the development and coordination of voluntary American national standards. American national standards for information systems are issued periodically by ANSI. Industry standards that the Air Force has adopted are published in the DoD Index of Specifications and Standards.

American Standard Code for Information Interchange (ASCII)—(1) The standard representation of numbers and letters by computers other than IBM (see also Extended Binary Coded Decimal Interchange Code). (2) The coded character set used for the general interchange of information among information processing systems and associated equipment. A standard code, using a coded character set consisting of 7-bit coded characters (8 bits including parity check), used for information interchange among data processing systems, data communication systems, and associated equipment. (a) ASCII Character Set: The ASCII 8-bit character set. It consists of the first 128 (0-127) characters of the ANSI character set. (b) ASCII Text. A subset of the ASCII, common to all computer devices, consisting principally of the printable characters.

Amplifier—An electrical or electronic device that increases the power or amplitude of a signal. The term amplifier typically implies a linear analog device that reproduces, at its output, a signal that is a linear replica of the input signal, but with a greater power or voltage level, and sometimes with an impedance transformation.

Amplitude Distortion—Distortion occurring in an amplifier or other electronic device when the

amplitude of the output is not a linear function of the input amplitude under specified conditions.

Amplitude Equalizer—A corrective network that is designed to make the amplitude characteristics of a circuit or system substantially equal over a desired frequency range.

Amplitude Modulation (AM)—A form of modulation in which the amplitude of a carrier wave is varied in accordance with the instantaneous value of the modulating signal.

Analog Data—Data represented as a physical quantity that is considered to be continuously variable and whose magnitude is made directly proportional to the data or to a suitable function of the data.

Analog—(1) A transmission mode in which information is encoded on a carrier wave by a continuously variable current or voltage level. (2) Pertaining to a device that measures a continuous variable (such as temperature on a thermometer) instead of indiscrete numbers.

Analytical Attack—An attempt to break a code or to find a key using analytical methods.

Anchor—A synonym for hyperlink. (A link in a given document to information within another document)

Angel Echoes—In radar, echoes that are obtained from regions of the atmosphere where there do not appear to exist any reflecting sources. Such reflections are primarily contributed to inhomogeneities in the refractive index of the atmosphere. Also called ghost echoes.

Anisynchronous—Pertaining to transmission in which the time interval separating any two significant instants in sequential signals is not necessarily related to the time interval separating any other two significant instants. (***NOTE***: Isochronous and Anisynchronous are characteristics, while Synchronous and Asynchronous are relationships.)

Annular Subclutter Visibility Photographs—Photographs that show how well a specific radar set tracks a target return of known electrical amplitude though ground clutter.

Anomalistic Period—In satellite communications, the time interval between two successive passages of a satellite through its apogee.

Anomalous Propagation—In radio communications, abnormal propagation due to discontinuities in the atmosphere and resulting, in many instances, in the reception of signals well beyond their normal range.

Answerback Data—A signal or tone sent by the receiving business machine or data set to the sending station for identification or to indicate it is ready to receive transmission.

Antenna—In communications-electronics, a frequency-sensitive device used to collect (receive) or radiate (transmit) electromagnetic (radio frequency) energy.

Antenna Squint—In radar, a characteristic where the actual position of the transmit beam varies with frequency both in azimuth and elevation. The de-squint circuitry in the radar processor is designed to compensate for this deviation.

Anthropomorphic Factors—Human body measurements involved with the design requirements of a system when the system is dependent upon humans for operation. Factors such as weight, height, arm reach, hand size, etc., become critical when designing operator stations, control panels, aircraft cockpits, etc..

Aperiodic Antenna—An antenna designed to have an approximately constant input impedance over a wide range of frequencies.

Aperture—(1) In computing, a part of a mask that permits retention of the corresponding portions of data. 2. In radio communications, the open end of a horn antenna.

Aperture Antenna—A microwave radio antenna employing a horn for a feed and reflector.

Aperture Blockage—In radar, an electrically opaque object that is located in front of the antenna and blocks the radiation distribution thereby distorting or shaping the beam pattern.

Apogee—The point in its orbit at which a satellite is at its maximum distance from the earth.

Application—A computer program that performs a specific function, such word processing, electronic mail, database management, etc. The term is used interchangeably with program.

Application Model—A term used to describe those functions of an organization that can be supported or automated through information technology (IT). Used for grouping or clustering functions into applications. It provides the application developers' views of the IT architecture.

Application Platform—The collection of hardware and software components that provide the services used by support and mission-specific software applications.

Application Portability Profile—The structure that integrates federal, national, international, and other specifications to provide the functionality necessary to accommodate the broad range of federal information technology requirements.

Application Program Interface (API)—(1) The interface between the application software and the application platform, across which all services are provided. The API is primarily in support of application portability, but system and application interoperability are also supported by a communications API. (2) A set of formalized software calls and routines that can be referenced by an application program to access underlying network services.

Application Software—Software that manipulates data, creates reports, performs calculations, and so forth. Word processing, database, graphics, and spreadsheet packages are examples of applications software.

Application Software Architecture—A framework for developing a software environment responsive to user information requirements.

Application Window—In computing, the window containing the work area and menu bar for an application. An application window may contain multiple document windows.

Appraisal—The process of determining the value and thus the final disposition of a record, making it either temporary or permanent. The National Archives and Records Administration is the only federal agency with the authority to appraise government records.

Architecture—There are different types of architectures, each with its own definition. The following are the DoD-approved definitions. (a) General Definition: A framework or structure that portrays relationships among all the elements of the subject force, subject, or activity. (b) The standard definitions for Operational, Systems, and Technical Architecture: Operational Architecture. A description of the tasks, operational elements, and information flows required to accomplish or support a war-fighting function. Systems Architecture. A description, including graphics, of the systems and interconnections providing for or supporting a war-fighting function. Technical Architecture. A minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements of a system, whose purpose is to ensure that a conformant system satisfies a specified set of requirements.

Arrester—In telecommunications, an electro-mechanical device that protects equipment and circuits from voltage or current surges produced by lightning or an electromagnetic pulse. Synonym: Surge Suppressor.

Artificial Intelligence Languages—Artificial intelligence languages are a subfield within computer science concerned with developing a technology to enable computers to solve problems (or assist humans to solve problems). They use explicit representations of knowledge and reasoning methods employing that knowledge.

Artificial Intelligence—The capability of a computer to perform functions that are normally attributed to human intelligence, such as learning, adapting, recognizing, classifying, reasoning, self-correction, and improvement.

Assembler—A computer program that translates symbolic codes into machine instructions, item for item.

Assembly—An item of equipment forming a portion of an end item of (communications) equipment and which item can be provisioned and replaced as an entity. An assembly normally incorporates replaceable parts or groups of parts.

Assigned Frequency—(1) The center frequency of a specified radiated bandwidth. (2) The center of the frequency band assigned to a station.

Assigned Frequency Band—The frequency band within which the emission of a station is authorized. The width of the band equals the necessary bandwidth plus twice the absolute value of the frequency tolerance. Where space stations are concerned, the assigned frequency band includes twice the maximum Doppler shift that may occur in relations to any point of the earth's surface.

Asynchronous Operation—An operation that occurs without a regular or predictable time relationship to a specified event; for example, the calling of an error diagnostic routine that may receive control at any time during the execution of a computer program. Also, a sequence of operations in which operations are executed but out-of-time coincidence with any event.

Asynchronous System—(1) A system employing start and stop elements for individual synchronization of each character information, or each word or block. The gaps between characters or words may be of variable length. (2) A data communications system that uses asynchronous operation. Synonym: Start-Stop System.

Asynchronous Transfer Mode (ATM)—A key broadband switching and transport technology that supports high-speed data, video, imaging, and voice applications as well as combinations of these in multimedia applications. ATM can do this as a multi-service platform using a single network rather than requiring separate networks specific to a service. It can send digitized information at more than 45,000 times the speed available on typical telephone lines. ATM is not an asynchronous transmission technique; transfer mode refers to the switching and multiplexing process.

Asynchronous Transmission—(1) A form of discontinuous data transmission that employs start and stop bits to signify the beginning and end of characters. Compare with Synchronous Transmission. (2) A transmission process such that between any two significant instants in the same group (in data transmission, this group is a block or a character) there is always an integral number of unit intervals. Between two significant instants located in different groups there is not always an integral number of unit intervals. (Also see Plesiochronous and Isochronous).

Atmospheric Duct—In electromagnetic propagation, a horizontal layer in the earth's lower atmosphere

in which the temperature and moisture gradients are such that the electromagnetic signals traveling within the layer (a) are guided or focused within the duct, (b) tend to follow the curvature of the earth, and (c) experience less attenuation in the duct than they would if the duct were not present. A strong temperature inversion and/or moisture lapse rate are necessary for the formation of a duct. Ducting may cause radio/ radar signals to be diverted from their intended path.

Attack—Intentional act of attempting to bypass one or more of the following security controls of an information system: nonrepudiation, authentication, integrity, availability, or confidentiality.

Attenuation—(1) The decrease in intensity of an electromagnetic signal as a result of absorption or reflection of energy due to the various characteristics of the path or circuit over which the signal is traveling. Attenuation is usually expressed in decibels. (2) A decrease in intensity of a signal, beam, or wave as a result of absorption of energy and of scattering out of the path of a detector, but not including the reduction due to geometric spreading (i.e., the inverse square of distance effect).

Atto (a)—A prefix used to denote one quintillionth (10^{-18})

Attributes—In reference to a communications system, the properties of discernible manifestations of the system and its components. These attributes characterize the parameters of a system.

Audio—(1) Generally refers to sound frequencies (tones) which can be heard by the human ear (usually between 20 hertz and 20,000 hertz). (2) Relating to recording, production, and reproduction of sound, especially the sound portion of a visual information production (for example, motion picture videotape, slide tape, etc.).

Audio Video Interleaved (AVI) (.avi)—In computing, a file-name extension used to indicate a compressed video file in the AVI standard for a common operating system.

Audiovisual (AV) Production—An AV production is distinguished from other visual information productions by the combination of motion media (for example, film, tape, or disk) with sound in a self-contained, complete presentation, developed according to a plan or script for the purpose of conveying information to, or communicating with, an audience.

Audit—Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Audit Trail—Chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event. Audit trail may apply to information in an Information System, to message routing in a communications system, or to the transfer of communications security material.

Augmented Reality (AR)—An area of virtual reality (VR). Unlike VR, AR does not strive for a totally immersive, 100% computerized environment, but puts helpful graphical data upon the real world view. For example, the projection of flight data onto an aircraft's windshield is a form of AR.

Authenticate—To verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an information system, or to establish the validity of a transmission.

Authenticator—(1) Means used to confirm the identity of a station, originator, or individual. (2) A symbol or group of symbols, or a series of bits, selected or derived in a prearranged manner and usually inserted at a predetermined point within a message or transmission for the purpose of attesting to the

validity of the message or transmission.

Authorized Bandwidth—The necessary bandwidth required for transmission and reception of intelligence. (Does not include allowance for transmitter drift or Doppler shift).

Auto-Manual System—In information assurance, programmable, hand-held cryptoequipment used to perform encoding and decoding functions.

Automated Data Processing (ADP)—An older term referring to the branch of science and technology concerned with methods and techniques relating to data processing largely performed by automatic means. Now largely replaced by the separate disciplines of Computer Science (for software) and Computer Engineering (for hardware).

Automated Data Processing Equipment (ADPE)—Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching interchange, transmission, or reception of data or information by a federal agency, or under contract with a federal agency that requires the use of such equipment, or requires the performance of a service, or the furnishing of a product that is performed or produced making significant use of such equipment. Such term includes computers; ancillary equipment; software, firmware, and similar procedures; services including support services; and related resources.

Automated Data Processing System (ADPS)—The total complement of all equipment, including computer hardware, firmware, software, communications equipment, and electronic devices designed to operate as an integrated system to achieve a desired data processing objective.

Automated Identification Technology (AIT)—A suite of technologies that facilitate the capture of information, such as bar codes, optical memory cards, magnetic strips, integrated circuit cards, radio frequency identification tags, movement tracking devices, and others. AIT can be used in a number of diverse environments and applications. The DoD uses AIT to enhance logistics business practices and provide status and location of its assets.

Automated Information System (AIS)—(1) An assembly of computer hardware, software, firmware, or any combination of these, configured to accomplish specific information-handling operations, such as communication, computation, dissemination, processing, and storage of information. (2) A combination of computer hardware/software, telecommunications, information technology, personnel, and other resources that collect, record, process, store, communicate, retrieve, and display information.

Automated Information Systems Security—See Information Systems Security.

Automated Security Monitoring—Use of automated procedures to ensure that security controls are not circumvented or the use of these tools to track actions taken by subjects suspected of misusing the information system.

Automated Tools—Software performing a sequence of operations to assist the user in achieving a goal (for example, within graphics software, functions that align objects, draw circles, etc.).

Automatic Calling Unit (ACU)—A dialing device supplied by the communication common carriers that permits a business machine to automatically dial calls over the communications network.

Automatic Clutter Filter (ACF)—In radar, a target extractor feature designed to control false alarms by eliminating slow moving targets.

Automatic Digital Network (AUTODIN)—A switched network of the Defense Information System

which functions as a single, integrated, worldwide, high-speed, computer-controlled, general-purpose communications network.

Automatic Link Establishment (ALE)—In high-frequency radio communications, (1) The capability of a station to make contact, or initiate a circuit, between itself and another specified radio station, without human intervention and usually under processor control. (2) A link control system that includes automatic scanning, selective calling, sounding, and transmit channel selection using link quality analysis data. Optional ALE functions include polling and the exchange of orderwire commands and messages.

Automatic Remote Rekeying—Procedure to rekey a distant cryptoequipment electronically without specific actions by the receiving terminal operator.

Automatic Secure Voice Communications (AUTOSEVOCOM)—A worldwide switched network designed to provide DoD users with secure voice communications within the Defense Information System.

Availability—In systems operations, a measure of the degree to which an item of equipment or a system is in the operable and committable state at the start of a mission, when the mission is called for at an unknown, random point in time. It is the probability that the system is operating satisfactorily at any point in time when used under stated conditions, where the total time considered includes operating time, active repair time, administrative time, and logistics time.

Back Lobe—A lobe of an antenna radiation pattern which is opposite the main lobe.

Background Noise—The total system noise in the absence of information transmission; it is independent of the presence or absence of a signal.

Backscatter (Wave)—In radio communications, an electro-magnetic wave produced as a result of scattering of the incident wave, through angles greater than 90o with reference to the original direction of travel.

Backward Channel—In data communications, a channel with a direction of transmission opposite to that in which user information is being transferred. Used for error control or supervisory channel.

Balanced—Electrically symmetrical with respect to ground. Also see Balanced Line.

Balanced Line—A transmission line consisting of two conductors in the presence of ground capable of being operated in such a way that when the voltages of the two conductors at all traverse planes are equal in magnitude and opposite in polarity with respect to ground, the currents in the two conductors are equal in magnitude and opposite in direction. Synonymous with Balanced Signal Pair.

Balun—Abbreviation for balanced to unbalanced. In radio communications, an electronic device for converting a balanced (transmission) line to an unbalanced line. Commonly used in high frequency (HF) radio systems.

Bandwidth—(1) The range of consecutive frequencies that comprise a band. (2) The difference, in Hz, between the lowest and highest frequencies of a signal or transmission. (3) In data communications it is loosely referred to as the amount of data that can be transferred over a network connection.

Base Communications—Facilities, equipment, and services used to communicate within the confines of a post, camp, station, base, headquarters, or federal building to include local interconnect trunks to the nearest commercial central office providing service to the local serving area. It also includes off-premise activity interconnections that are located within the geographical boundary served by the connecting

commercial central office.

Base C4 Systems Blueprint—The base Systems Telecommunications Engineering Manager's product that documents the C4 systems' baseline, identifies a target base configuration to support present and future requirements of the base, and provides a time-phased plan for logical transition from the baseline to the target configuration.

Base Level C4 Infrastructure—The common-user portion of the base-level C4 systems environment. It includes transmission, switching, processing, system control, and network management systems, equipment, and facilities which support the base as a whole. Examples include the base telephone switches and cable plant, base communications center, network control center, and metropolitan area network (also known as "base communications infrastructure").

Base Station—A land station in the land mobile radio service.

Baseband—In radio communications, the aggregate band of frequencies in a radio transmitter prior to modulation. The baseband signal is usually used to modulate the carrier. Demodulation in the radio receiver recreates the baseband signal. The baseband signals represent the intelligence information transmitted over the radio system. The "baseband" (in baseband frequencies) is used as an adjective to distinguish from radio frequencies (RF).

Baseline—A specification or product that has been formally reviewed and agreed upon, that serves as a basis for further development, and that can be changed only through formal change control procedures or a type of procedure such as configuration management.

Baseline Configuration—A configuration that consists of an inventory of information resources (that is, hardware, software or data, or any combination thereof) currently operational within the organization.

Basic Input/Output System (BIOS)—A program stored in read-only memory and accessed automatically each time the system is turned on. It checks the configuration data and performs self-tests to make sure the system is functional. When the checking is complete, the program loads and turns control over to the operating system.

Basic Software—Comprises those routines and programs designed to extend or facilitate the use of particular automated data processing equipment, the requirement for which takes into account the design characteristics of such equipment. This software is usually provided by the original equipment manufacturer (OEM) and is normally essential to, and a part of, the system configuration by the OEM. Examples of basic software are executive and operating programs; diagnostic programs; compilers; assemblers; utility routines, such as sort/merge and input/output conversion routines; file management programs; and data management programs. Data management programs are commonly linked to, or under the control of, the executive or operating programs.

Basic Telecommunications Services—The Federal Communications Commission's definition of common carrier transmission services which only result in the movement of information and do not involve the manipulation or restructuring of such information.

BASIC—Acronym for Beginner's All-purpose Symbolic Instruction Code. A widely adapted programming language that uses English words, punctuation marks, and algebraic notation to facilitate communication between the operator or layperson and the computer. A common programming language used on many minicomputers.

Batch Processing—Processing data or the accomplishment of jobs accumulated in advance in such a

manner that each accumulation formed is processed or accomplished in the same computer run.

Batched Communication—The transmission of a large body of network data from one station to another without intervening responses from the receiving unit.

Baud—A unit of signaling speed in data transmission equal to the number of discrete conditions or signal events per second. One baud corresponds to a rate of one unit interval per second where the modulation rate is expressed as the reciprocal of the duration in seconds of the unit interval. For example, if the duration of the unit interval is 20 milliseconds, the modulation rate is 50 baud.

Baudot Code—A code for the transmission of data in which five equal-length bits represent one character. In teletypewriter applications, a stop and start element are added to each character.

Beacon (satellite)—In satellite communications, a discrete radio frequency (RF) transmitted by the satellite for the purpose of tracking (of the satellite) by the earth station antenna system. The beacon RF signal is modulated by an identification frequency (tone).

Beam—In radio frequency wave propagation, the main lobe of the radiation pattern of a directional antenna.

Beamsplit—In radar, a method to determine the target center relative to the beam's position.

Beamspoiling—In radar, a technique to broaden the beams in elevation at high angles to obtain more vertical coverage.

Beamwidth—In radio communications, the angle (in degrees) between the half-power points (3 dB points) of the main lobe of the antenna pattern when referred to the peak power point of the antenna pattern.

Benign—A condition of cryptographic data that cannot be compromised by human access.

Beta Test—Second stage in the testing of computer software before the commercial release. Tests are usually conducted outside the company manufacturing the software.

Beyond A1—Level of trust defined by the DoD Trusted Computer System Evaluation Criteria to be beyond the state-of-the-art technology. It includes all the Al-level features plus additional ones not required at the Al-level.

Bias—(1) The amount by which the average of a set of values departs from a reference value. (2) A systematic deviation of a value from a reference value. (3) Electrical, magnetic, mechanical, or other force (field) applied to a device to establish a reference level to operate the device.

Bifurcation—A condition where only two outcomes are possible (for example, on and off, 0 and 1).

Billboard Antenna—An array of parallel dipole antennas with flat reflectors, usually positioned in a line or plane. Synonym: broadside antenna.

Binary Code—A code composed by selection and configuration of an entity that can assume either one of two possible states.

Binary Digit (Bit)—(1) In pure binary notation, either of the characters 0 or 1. (2) A unit of information equal to one binary decision or the designation of one of two possible and equally likely states of anything used to store or convey information.

Binary File—A file containing characters that are in machine-readable form.

Binary Modulation—The process of varying a parameter of a carrier as a function of two finite and discrete states.

Binary Number—A number expressed in binary notation.

Binding—Process of associating a specific communications terminal with a specific cryptographic key or associating two related elements of information.

Biometrics Technologies—Automated methods of identifying or authenticating the identity of a living person based on a physical or behavioral characteristic. Unique physical traits, such as fingerprints, iris scan, voiceprint, facial recognition, signature verification, wrist veins, or the geometry of the hand or a finger, etc., can be used. These technologies work by comparing a registered or enrolled biometrics sample against a newly captured biometrics sample.

Bipolar—Pertaining to a system that undertakes both positive and negative values.

Bipolar Signal—An electrical signal that may assume either of two polarities, neither of which is zero. A bipolar signal is usually symmetrical with respect to zero amplitude (that is, the absolute values of the positive and negative signal states are nominally equal).

Bit—A contraction of the term Binary Digit. The smallest unit of information in a binary system of notation. A bit can be one of only two states, on (usually designated as 1) or off (usually designated as 0). Bits are grouped into bytes (usually 8 bits). Computer memory capacity is stated in the number of bytes that can be stored.

Bit Error Rate (BER)—The number of erroneous bits divided by the total number of bits over some stipulated period of time. The BER is usually expressed as a number and a power of 10 (for example, 5 in 10-^{6}).

Bit Stuffing—(1) A synchronization method used in time division multiplexing to handle received bit streams over which the multiplexer clock has no control. (2) The insertion of noninformation bits into data. Bit stuffing is used for various purposes, such as for synchronizing bit streams, or to fill buffers or frames.

Biternary Transmission—A method of digital transmission in which two binary pulse trains are combined for transmission over a system in which the available bandwidth is only sufficient for transmission of one of the two pulse trains when in binary form. The biternary signal is generated from two synchronous binary signals, operating at the same bit rate. Each biternary signal element can assume any one of three possible states: +1, 0, or -1.

Bitmap—An image stored as an array of bits.

Bit-Mapped Display—Display in which every picture element (pixel) of the screen can be referenced individually.

Black—A designation applied to telecommunications systems, and associated areas, circuits, components, and equipment, in which national security information is not processed.

Black Key—Encrypted key. See Red Key.

Black Line—In telecommunications, a transmission line which carries only unclassified or enciphered signals.

Black Signal—In telecommunications, any enciphered or control signal that would not divulge national

security information if recovered and analyzed.

Blanking Angels—In radar, boundary azimuths at the radar, which prevent the transmitter from radiating into areas where radiation hazards or interference would occur.

Blind Speeds—In radar, certain radial ground speeds, relative to the radar, which cause the radar to see objects as being stationary. Such targets are cancelled by the moving target indicator (MTI) receiver and are not processed for display.

Bluetooth Radio Technology—(1) A global specification for short-range wireless connectivity that enables portable and stationary communications devices to operate over a distance of 10 meters. It provides a universal bridge to data networks. Designed to work in a noise radio frequency environment, it uses a fast acknowledgement and frequency-hopping scheme. Bluetooth technology involves a chip with a miniature radio transmitter/receiver attached that can relay information between devices without being connected by cables. (2) Bluetooth is a method for data communication that uses short-range radio links to replace cables between computers and their units. Bluetooth is by its nature not designed to carry heavy traffic loads; it is not suitable for replacing local or wide area networks and backbone cables.

Boundary—Software, hardware, or physical barrier that limits access to a system or part of a system.

Boresight—(1) The central axis of the main lobe of a directional antenna radiation pattern, or the central axis about which the lobes of a multi-lobe pattern are symmetrically positioned. (2) The process of establishing the actual electrical beam center with respect to a mechanical indicator (boresight error).

Branching Menu—A menu that, if selected, brings up another menu.

Breach—The successful defeat of security controls, which, if carried to consummation, could result in a penetration of an automated information system.

Bridge—(1) In data communications, a device that provides connection between two local area networks using the same logical link control procedure, but may use different medium access control procedures. (2) A balanced electrical network; a bridge may be used for electrical measurements such as resistances or impedances.

Broadband—In today's C4 environment, broadband is an imprecise term having different meanings in different applications, but in general refers to connections handling more than 1 million bits of information per second. Synonymous with wideband.

Broadband Communications Bus (BCB)—A concept for linking non-cockpit airborne communications through a high capacity local area network-like backbone. Information devices may be voice, video, or data, and are connected to a wide array of communications channels, including UHF SATCOM, HF radio and telephone, both while on the ground and in the air.

Broadcast—(1) In data communications, a method of message routing in which the message is transmitted to all nodes in the network. (2) In radio communications, the simultaneous transmission of a signal or message to a number of stations. This is typically a one-way transmission only and does not involve a response to the originator of the transmission.

Broadcasting Service—A radio communications service in which the transmissions are intended for direct reception by the general public. This service may include sound, television, or other types of transmissions.

Broadside—Antenna See billboard antenna.

Brouter—A combined bridge and router that operates without protocol restrictions. Routes data using a protocol it supports, and bridges data it cannot route.

Browser—(1) Any computer software program for reading hypertext. (2) A World Wide Web (WWW) client tool used to retrieve information from the WWW.

Browsing—The act of searching through a communications and information system storage to locate or acquire information without necessarily knowing of the existence or the format of the information being sought.

Bubble Memory—A solid state storage device using microscopic magnetic domains in an aluminum garnet substrate. The domains, or bubbles, are circulated within the substrate and are directed to the output by magnetic fields. This technology has the advantage over random-access memory in that it is non-volatile.

Buffer—(1) A routine or storage used to compensate for the difference in rate of flow of data, or time of occurrence of events, when transferring data from one device to another. (2) An isolating circuit used to prevent a driven circuit from influencing the driving circuit. (3) To allocate and schedule the use of buffers.

Built-in Test Equipment (BITE)—In communications-electronics, an electrical or electronic device permanently mounted in the prime equipment and used for the express purpose of testing the prime equipment, either independently or in association with external test equipment.

Bulk Item—In logistics, bulk items are support items that are normally not supplied or used as individual piece parts. Examples are: sheet metal, wire, paints, lubricants.

Bulk Encryption—Simultaneous encryption of all channels of a multichannel telecommunications link.

Burn-In Period—A term used to describe a process during which failures of new equipment items or component parts are likely to occur more frequently. The equipment is operated under power for a period called burn-in to eliminate weak components. Items that successfully survive the burn-in will likely perform satisfactorily for extended periods.

Burnthrough Range—In radar, the range at which the strength of the radar echoes becomes greater than the strength of an interfering or jamming signal.

Burst—In data communications, a sequence of signals, noise, or interference counted as a unit in accordance with some specific criterion or measure.

Burst Transmission—(1) A transmission that combines a very high data signaling rate with very short transmission times. (2) Operation of a data network in which data transmission is interrupted at intervals.

Bus—(1) In communications-electronics, one or more conductors that serve as a common connection for a related group of devices. (2) In a computer, an electronic path for sending data from one part of the computer to another part or to an external device. There are two buses within the Central Processor Unit (CPU): the address bus and the data bus. The address bus connects the CPU and memory. The data bus allows connection with external equipment and is identified primarily by its width, measured in bits (8, 16, 32, etc.). The wider the bus path, the higher the “speed” of the computer.

Byte—A sequence of eight consecutive bits (normally 8), usually shorter than a word, operated on as a unit.

C—An intermediate programming language, in some respects similar to an assembly language, but with

many features that support structured programming.

C Band—In radio communications, the frequency band between 4-8 GHz.

Cable Television (CATV) System—Distributes one or more television programs by modulated radio frequency or other signals through a cable distribution system to standard television or radio receivers.

Cache (Memory)—In computing, memory location set aside to store frequently accessed data for improved system performance. This is a high-speed buffer random access memory (RAM) used between the central processor and main memory. It is used to reduce hard disk access time by storing the commands needed to operate the hard disk.

Call Back—Procedure for identifying and authenticating a remote communications system terminal, whereby the host system disconnects the terminal and re-establishes contact. Synonymous with Dial Back.

Call Second—A unit of communications traffic, such that one call-second may be defined as a one-second call made by one user.

Call Sign—In radio communications, any combination of numbers, letters, or pronounceable words, which identify a communications platform, facility, station, unit, or individual. Used primarily to establish and maintain communications.

Campus Area Network (CAN)—Generally considered as the next level in scale of operation to the Local Area Network (LAN), a CAN is an interconnected series of LANs within a contiguous area. Within the DoD, this is most often aligned with the network environment contained within the boundary of a post, camp, or station.

Capability Maturity Model (CMM)—A framework that describes the elements of an effective software process. It describes an evolutionary improvement path toward a disciplined process.

Capacity—(1) In computing, the total number of bytes that can be stored in memory or a disk; the value may be given as either the unformatted or formatted size. (2) In satellite communications, the communications throughput and/or number of accesses provided by a satellite system.

Capstone Requirements Document (CRD)—A document that contains capabilities-based requirements that facilitates the development of individual Operational Requirements Documents (ORDs) by providing a common framework and operational concept to guide their development. It is an oversight tool for overarching requirements for a system-of-systems or family-of-systems.

Capture Effect—In radio communications, the effect associated with the reception of frequency modulated signals in which, if two signals are received on the same frequency, only the stronger of the two will appear in the output of the radio receiver.

Card—In electronics, a flat piece of hardware containing electrical and electronic components on a fiberglass or plastic foundation. Cards are designed to perform a wide variety of functions in communications and computer equipment.

Carrier Frequency—(1) The frequency of a carrier wave. (2) A frequency capable of being modulated or impressed with a second (information carrying) signal. (3) In frequency modulation, the carrier frequency is also referred to as the center frequency.

Carrier Power—In an amplitude modulated radio system, the average power supplied to the antenna transmission line by a radio transmitter during one radio frequency cycle under conditions of no

modulation.

Carrier Sense Multiple Access (CSMA)—In data communications, a method of providing multiple access to a shared channel in which all stations employ a listen-before-talk transmission logic.

Carrier—(1) An electromagnetic signal frequency suitable for modulation by an intelligence-bearing signal to be transmitted over a communications system. (2) An unmodulated radio frequency emission.

Cascading—In communications security, a downward flow of information across a range of security levels that is greater than the accreditation range of a component part of a network.

Cassegrain Antenna—In radio communications, a type of dish antenna in which a small reflector is mounted at the focal point. The received signals are first reflected by the antenna to this reflector and then reflected once more into the feedhorn mounted at the center of the dish.

Cellular Radio Telephone System—A computer-controlled full duplex telephone service linking low-power portable, mobile, or porta-mobile radio-telephone transceivers to a local telephone switch. The principal feature is the ability to separate and reuse a limited number of radio frequencies in a large network of relatively small geographic cells. Frequencies for telephones moving between adjacent cells often shift to avoid interference with frequencies of other calls.

Cellular Telephone—A portable telephone in a cellular radio system.

Centi (c)—A prefix denoting one hundredth (10^{-2}).

Central Exchange (CENTREX)—A type of private branch exchange service in which incoming calls can be dialed direct to any extension without an operator's assistance. Outgoing and intercom calls are dialed direct by the extension users. It is the partitioning of a local exchange carrier switch to provide intrapremise dialing with an abbreviated dialing plan and trunking to external networks.

Central Office—(1) In telephone communications, a common carrier switching center which houses the necessary equipment and operations to switch and terminate subscriber lines and trunks. (2) In a telephone system, a switching unit which provides service to the general public. There may be more than one central office in a building. Some (loosely used) synonyms for central office are: exchange, local exchange, telephone exchange, local office, end office.

Central Office of Record (COR)—A federal department or agency office that keeps records of accountable communications security material held by activities it oversees.

Central Office Trunks—Trunks from the base telephone system to the local telephone company central office. Trunks connect telephones on base to those in the commercial exchange.

Central Processing Unit (CPU)—The portion of a computer that executes programmed instructions, performs arithmetic and logic functions, and controls input and output functions. One CPU may have more than one processor housed in the unit.

Centralized Control—In satellite communications, refers to a principle architectural objective that provides the centralized timing, resource allocation, and orderwire functions required to automatically share satellite resources among users.

Certificate—A record holding security information about a communications system's user; it vouches to the truth and accuracy of the information it contains.

Certificate of Action Statement—A statement attached to a communications security audit report by which a communications security custodian certifies that all actions have been completed.

Certificate of Networthiness (CON)—A document signed by the AF-CIO (or MAJCOM CIO) certifying that a system or application has satisfactorily completed a networthiness assessment, and: (1) will not harm the enterprise network; (2) information assurance needs have been adequately addressed; (3) spectrum is available and specifically allocated; and (4) quantitative and qualitative trained personnel requirements are met--before the system is fielded.

Certificate Revocation List—A time-stamped list of revoked certificates that has been digitally signed by a certification authority.

Certificate to Operate (CTO)—A document signed by the MAJCOM CIO certifying that a system or application has been successfully assessed to determine: (1) the adequacy of support planning, training, and implementation to mitigate potential fielding problems, provide effective enterprise management; and (2) reduce life-cycle costs.

Certification—A comprehensive, fully documented evaluation of the technical and non-technical security features of an information system and other safeguards made in support of the accreditation process. When this documented level of protection and/or risk is considered to be acceptable by the designated approving authority the system accreditation can take place.

Certification and Accreditation—In computing, the formal process implementing risk management. It includes risk analysis, certification, and accreditation.

Certification Authority (CA)—Third level Public Key Infrastructure (PKI) Certification Management Authority responsible for issuing and revoking user certificates, and exacting compliance to the PKI policy as defined by the parent Policy Creation Authority.

Certification Authority Workstation (CAW)—A commercial-off-the-shelf workstation with a trusted operating system and special purpose application software that is used to issue certificates.

Certification Level—A measure of the level-of-effort required to certify and accredit an information system. It identifies the required certification steps and the minimum documentation, tests, and reports. The certification level is calculated using the degrees of assurance.

Certification Package—Product of the certification effort documenting the detailed results of the certification activities.

Certification Test And Evaluation (CT&E)—Software and hardware security tests conducted during development of an Information System.

Certified Technical Solution—A detailed and costed description of a C4 system requirement that can be incorporated into the base infrastructure and is compliant with downward directed architectures and standards.

Certified Tempest Technical Authority (CTTA)—An experienced, technically qualified U.S. Government employee who has met established certification requirements in accordance with National Telecommunications and Information System Service Center-approved criteria and has been appointed by a U.S. Government Department or Agency to fulfill CTTA responsibilities.

Certifying Official—Individual responsible for making a technical judgment of the automated information system's compliance with stated security requirements and requesting approval to operate from the designated approval authority.

Channel—(1) In telecommunications, a physical or logical path allowing the transmission of

information; the path connecting a data source and a data sink, or receiver. (2) The smallest subdivision of a carrier system by which a single type of communications service is provided (e.g., voice channel, data channel).

Channel Bank—Equipment, typically in a telephone central office, that performs multiplexing of lower speed, generally digital, channels into a higher speed composite channel. The channel bank detects and transmits signaling information for each channel, and transmits framing information so that time slots allocated to each channel can be identified by the receiver.

Channel Packing—A technique for maximizing the utilization of voice frequency signals used for data transmission by multiplexing a number of low speed data signals into a single higher speed data stream for transmission on a single voice frequency channel.

Channel Controller—In satellite communications, the equipment that generates, receives, and processes orderwires.

Character—Any number, letter, punctuation mark, or space.

Character Set—A group of letters, numbers, and symbols that have some relationship in common. For example, the American Standard Code for Information Interchange (ASCII) character set contains characters that make up the ASCII coding.

Characteristic Frequency—A frequency that can be easily identified and measured in a given emission. A carrier frequency may, for example, be designated as the characteristic frequency (see also Reference Frequency).

Characters Per Second (CHPS)—A measure of data transmission rate, usually between a terminal device and a computer.

Check Bit—A binary digit derived from and appended to a data item, for later use in error detection and possibly error correction.

Check Word—In communications security, cipher text generated by a cryptographic logic to detect failures in the cryptography.

Chief Information Officer (CIO)—As mandated by Public Law 104-106, *Subdivision E of the Clinger-Cohen Act of 1996* (formerly the Information Technology Management Reform Act [ITMRA] of 1996), the CIO is an official who is appointed by the head of an executive agency, and is assigned overall responsibility to improve the agency's acquisition and use of information and information technology. In the Air Force, SAF/AQ is appointed as the AF-CIO.

Cipher—(1) A cryptographic algorithm; a mathematical function for encryption and decryption. (2) Any cryptographic system in which arbitrary symbols or groups of symbols, represent units of plain text or in which units of plain text are rearranged, or both. (3) A symbol, as a letter or number, that represents information.

Cipher Text—Enciphered information.

Cipher Text Auto-Key—Cryptographic logic which uses previous cipher text to generate a key stream.

Ciphony—The electronic scrambling of voice transmissions, resulting in encrypted speech.

Circuit—(1) A communications link between two or more points. (2) An electronic path between two or more points capable of providing a number of channels. (3) A number of conductors connected together for the purpose of carrying an electrical current. (4) The complete path between two end terminals over

which one-way or two-way communications may be provided.

Circuit Switching—A networking technique where the source and destination are connected by an exclusive communications path that is established at the beginning of the transmission and broken at the end.

Civil Satellite Communications—Satellite communications which are owned by or operated for non-DoD agencies.

Classified Cryptographic Information—Classified cryptographic media that embody, describe, or implement a classified cryptographic logic, including depot-level maintenance manuals, cryptographic descriptions, drawings of cryptographic logic, specifications describing a cryptographic logic, and cryptographic computer software.

Classified Information—(1) Information that has been determined pursuant to Executive Order 12958 or any predecessor order, or by the *Atomic Energy Act of 1954*, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status. (2) Official information that has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated.

Clearing—Removal of data from a communications and information system, its storage devices and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capabilities.

Client—In computer networking, (1) The software that allows users to retrieve information or services from the Internet and World Wide Web. (2) A personal computer workstation, connected to a network, which can access data or programs from the server computer. (3) A node that requests network services from a server.

Client/Server Interface—A software program that provides an interface to remote programs (called clients), most commonly across a network, to provide these clients with access to some service such as databases, printing, etc. In general, the clients act on behalf of a human end-user.

Client/Server Model—An architectural model for distributed computing environments. The model identifies two components: clients and servers. Clients are processes that request services and servers are processes that perform services. The client/server model provides the most consistent path to achieve a distributed computing environment capable of supporting the information technology. The client/server model insulates the client from how and where services are provided.

Clinger-Cohen Act of 1996—Public Law 104-106, *Subdivision E of the Clinger-Cohen Act of 1996*, February 10, 1996 (formerly the Information Technology Management Reform Act [ITMRA] of 1996). The Federal act which repealed the Brooks Act and rescinded the Federal information resources management regulations (FIRMR), and superseded them as the primary Federal guidance on information technology acquisition and management. Among other provisions, it renamed Federal information processing (FIP) resources as information technology (IT); transferred overall responsibility for acquiring and managing Federal IT from the General Services Administration (GSA) to the Office of Management and Budget (OMB); it gave IT procurement authority back to the individual agencies; and called for agencies to establish chief information officers (CIO) and participate in an interagency CIO council.

Clipboard—A temporary storage location in a small computer used to transfer data between documents and between applications. Typically, data is transferred to the clipboard by using an application's copy or cut command; data is transferred from the clipboard by the paste command.

Clock—A reference source of timing information for a machine, system, or equipment.

Clocking—A reference source of timing for a machine or system.

Closed Circuit—(1) A term used in radio and television transmissions to indicate that the programs are transmitted directly to specific users and not broadcast for general consumption. (2) A complete electrical circuit.

Closed Security Environment—In communications security, an environment that provides sufficient assurance that applications and equipment are protected against the introduction of malicious logic before or during the operation of a system.

Closed System—A communications system that does not interact significantly with its environment. The environment only provides a context for the system. Closed systems exhibit the characteristics of equilibrium resulting from external rigidity that maintains the system in spite of influences from the environment.

Clutter—In radar, the unwanted signals, echoes, or images on the radar display that are interfering with the observation of desired signals.

Coaxial Cable—An electrical cable consisting of a center conductor surrounded by an insulating material and a concentric outer conductor. Coaxial cable is primarily used for video, wideband, and radio frequency applications.

Co-Channel Interference—Interference resulting from two or more transmissions on the same channel.

Code Book—In communications security, a book or other document containing plain text and its code equivalents in a systematic arrangement, or a technique of machine encryption using a word substitution technique.

Codebook Excited Linear Predictive (CELP)—In Voice over Internet Protocol (VoIP), a speech compression method that achieves high compression ratios for toll quality voice.

Code Group—In communications security, a group of letters, numbers, or both, in a code system used to represent a plain text word, phrase, or sentence.

Code Vocabulary—Set of plain text words, numerals, phrases, or sentences for which code equivalents are assigned in a code system.

Code—(1) System of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length. (2) A cryptosystem in which the cryptographic equivalents (usually called “code groups”) typically consisting of letters or digits (or both) in otherwise meaningless combinations are substituted for plain text elements which are primarily words, phrases, or sentences. See also cryptosystem.

Coder/Decoder (CODEC)—A device that converts analog signals to digital form for transmission over a digital network and conversion back to their original analog form.

Coercivity—Amount of applied magnetic field (of opposite polarity) required to reduce magnetic induction to zero. Coercivity is measured in oersteds (Oe). It is often used to represent the relative difficulty of degaussing various magnetic media.

Cognizant Security Authority (CSA)—An individual, usually at the MAJCOM level, who is authorized to make communications security policy decisions based on current Air Force communications security doctrine.

Cold Boot—Procedures performed to load a computer's operating system software following a power-up. Also, the process of trying to clear a perceived problem from a system by deliberately turning a computer device off and back on.

Cold Start—Procedure for initially keying cryptoequipment.

Collaborative Tools—A suite of hardware and software that allows multiple users in various locations to meet in a virtual environment to simultaneously and collectively exchange information and to share software applications and electronic files in a real time or near real time environment.

Collateral Information—All national security information classified under the provisions of an executive order, for which special community systems of compartments (for example, sensitive compartmented information) are not formally established.

Color Graphics Array (CGA)—A type of video display unit.

Combat Camera (COMCAM)—Visual information documentation covering air, ground, and sea actions of armed forces in combat and combat support operations and in related peacetime training activities such as exercises, war games, and operations.

Combat Information Transfer System (CITS)—A high speed, high bandwidth information transport system that links facilities with existing and planned voice, data, video, and imagery systems via a fiber optics switch asynchronous transfer mode (ATM) network.

Combiner—In telecommunications, an electronic device employed in wideband radio receiving equipment that compares or combines signals received over different radio paths and selects the signal with the better signal-to-noise ratio, thus ensuring the best available quality of communications under the prevailing conditions.

Command and Control (C2)—The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.

Command and Control Support (C2S) System—The C2S system is the primary means through which the joint force commander (JFC) and subordinate warriors control the flow and processing of information. The C2S system allows the JFC to control the flow and processing of information to support decision-making and influence action during the execution of joint operations.

Command and Control Warfare (C2W)—The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information, to influence, degrade or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such action. Command and control warfare is an application of information operations and is both offensive and defensive.

Command Authority—Individual responsible for the appointment of user representatives for a department, agency, or organization and their key ordering privileges.

Command Communications Service Designator (CCSD)—In the Defense Information Systems Network (DISN), an eight digit alpha-numeric code assigned to each communications circuit and which identifies the agency requiring the service, purpose and use, category of service, and unique circuit number.

Command, Control, Communications, and Computer (C4) System—An integrated system of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control across the range of military operations. (DoD). Also called communications and information system in the Air Force.

Command, Control, Communications, Computers Infostructure—The shared computers, ancillary equipment, software, firmware and similar procedures, services, people, and related resources used in the acquisition, storage, manipulation, protection, management, movement, control, display, switching, interchange, transmission, or reception of information or information in any format including audio, video, imagery, or data, whether supporting Information Technology (IT) or National Security systems as defined in the Clinger-Cohen Act of 1996.

Command, Control, Communications, Computers, and Intelligence (C4I) Interoperability Steering Group (ISG)—The C4I ISG consists of O-6 level members from the office of the Secretary of the Air Force, Air Staff, major air commands (MAJCOM), and field operating agencies (FOA). The C4I ISG promotes the interoperability of C4I systems in the Air Force.

Command Language—In programming, a source language consisting principally of procedural operations, each capable of invoking a function to be executed.

Commercial And Non-Developmental Item (CANDI)—A term used when referring to both commercial and non-developmental items.

Commercial communications security (COMSEC) Endorsement Program (CCEP)—Relationship between the National Security Agency and industry, in which the National Security Agency provides the COMSEC expertise (i.e., standards, algorithms, evaluations, and guidance) and industry provides design, development, and production capabilities to produce a type 1 or type 2 product. Products developed under the CCEP may include modules, subsystems, equipment, systems, and ancillary devices.

Commercial Communications—The circuits, services, equipment, and facilities furnished by the private sector (regulated and non-regulated entities) or foreign communications entities that satisfy telecommunications requirements.

Commercial Item—Any item, other than real property, of a type customarily used for non-government purposes and that has been sold, leased, or licensed to the general public; or has been offered for sale, lease, or license to the general public; or any item evolved through advances in technology or performance and that is not yet available in the commercial marketplace, but will be available in the commercial marketplace in time to satisfy the delivery requirements under a government solicitation. Also included in this definition are services in support of a commercial item, of a type offered and sold competitively in substantial quantities in the commercial marketplace based on established catalog or market prices for specific tasks performed under standard commercial terms and conditions; this does not include services that are sold based on hourly rates without an established catalog or market price for a specified service performed.

Commercial Satellite Communications—Satellite communications resources provided by commercial companies or organizations using commercial frequencies.

Commercial Multimedia (MM) Production—A completed MM production, purchased off the shelf, from the stocks of a vendor.

Commercially Procurable Work—Printing and binding work that may be obtained through the Defense Printing Service or the Government Printing Office commercial sources, within the customer's time frame

and without compromising security.

Commercial-Off-The-Shelf (COTS) Products—(1) Hardware and software products developed, tested, and sold by commercial companies to the general public. (2) Commercial items that require no unique government modifications or maintenance over the life cycle of the product to meet the needs of the procuring agency.

Commodity—Under the lead operating command concept, a commodity is an equipment item within a specified group or category of communications and information equipment. Items within a specific group basically possess similar operational characteristics, have similar applications, and are susceptible to similar life-cycle management methods. Examples of commodities are desktop computers, land mobile radios, pagers, telephones, cellular telephones, etc.

Common Applications Environment (CAE)—The X/Open term for a computer environment in which applications can be ported across X/Open vendor systems. It includes standards for the operating system, languages, networking protocols, and data management.

Common Battery—In telephony, a dc power source in the central office that supplies power to all subscriber stations and central office switching equipment.

Common Carrier (CC)—A private company, subject to government regulation (Federal Communications Commission and state), that furnishes the general public with telecommunications services (for example, a telephone or satellite communications company).

Common Channel Signaling (CCS)—In telecommunications, the exchange of information between switches for all setup and supervision, status monitoring, network management, etc., using separate, dedicated, high-speed data links.

Common Fill Device—One of a family of devices developed to read-in, transfer, or store key.

Common Gateway Interface (CGI)—A set of rules that describe how a Web server communicates with another software program (the CGI program) on the same machine and how the CGI program talks to the Web server. Any software program can be a CGI program if it handles input and output according to the CGI standard.

Common Operating Environment (COE)—The COE provides an approved set of standards that defines the interfaces, services, protocols, and supporting formats required for application portability profiles. The COE integrates numerous elements (building blocks) that make up the total network or system and is the key element of interoperability. The COE provides a familiar look, touch, sound, and feel of the C4I environment to the warrior, no matter where the warrior is employed. Information presentation and C4I system interfaces are maintained consistently from platform to platform, enabling the warrior to focus attention on the crisis at hand.

Common User Circuit—A circuit designated to furnish a communication service to a number of users.

Common User Network—A system of circuits or channels allocated to furnish communication paths between switching centers to provide communication service on a common basis to all connected stations or subscribers. It is sometimes described as a general-purpose network.

Commonality—A quality that applies to materiel or systems possessing like and interchangeable characteristics enabling each to be used, or operated and maintained, by personnel trained on the others without additional specialized training; having interchangeable repair parts and, or components; and applying to consumable items interchangeably equivalent without adjustment.

Communications—A method or means of conveying information of any kind from one person or place to another.

Communications and Information—The consolidated Air Force functional area that includes telecommunications, computers, information management, and audiovisual information. In the Air Force, the term Communications and Information is the equivalent of C4. There is no approved acronym for Communications and Information.

Communications and Information Mission Support Plan—The guide for acquiring, using, and disposing of communications and information systems. A key feature of this plan is the way it links those systems to the missions and functions of the Air Force. The plan puts communications and information systems in operational context, and it presents an information system investment strategy that will result in air and space forces that work better and cost less.

Communications and Information System—An integrated system of communications equipment (hardware and software), facilities, personnel, and procedures designed to provide communications and information to its users. This includes the processing of the information by the system. Communications and information systems include base visual information support systems. Also called Command, Control, Communications and Computer (C4) system.

Communications and Information System Blueprint—A base level plan, produced by the base-level systems telecommunications engineering manager (STEM-B), that outlines each Air Force base's existing and targeted communications and information systems. It is the configuration, management, and control document for the base communications infrastructure. It covers the existing infrastructure baseline, on-going communications programs and projects, short- and long-range planned systems, and identifies estimated resources required. It is and documents the baseline, identifies a target base configuration to support present and future requirements, and provides a time-phased plan and estimated costs for the logical transition from the baseline to the target configuration.

Communications and Information Systems Officer (CSO)—The officer responsible for communications and information systems and functions at any Air Force organizational level. At base level, the base CSO is the commander of the communications unit. At the MAJCOM level, the MAJCOM CSO is designated by the MAJCOM commander.

Communications and Information Systems Security—The protection afforded to communications and information systems to preserve the availability, integrity, and confidentiality of the systems and the information contained within the systems. Such protection is the integrated application of communications security, TEMPEST, and COMPUSEC.

Communications Deception—Use of devices, operations, and techniques with the intent of confusing or misleading the user of a communications link or a navigation system.

Communications-Electronics—The specialized field concerned with the use of electronic devices and systems for the acquisition or acceptance, processing, storage, display, analysis, protection, disposition, and transfer of information.

Communications Link—The cables, wires, or paths that the electrical, optical, or electromagnetic (radio) wave signals traverse between a transmitting (sending) and receiving station.

Communications Network—(1) An organization of stations capable of intercommunications, but not necessarily on the same channel. (2) A set of products, concepts, and services which enables the connection of computer systems for the purpose of transmitting data and other forms (for example, voice

and video) between the systems.

Communications Node—A node that is either internal to the communications network (for example, routers, bridges, or repeaters) or located between the end device and the communications network to operate as a gateway.

Communications Profile—Analytic model of communications associated with an organization or activity. The model is prepared from a systematic examination of communications content and patterns, the functions they reflect, and the communications security measures applied.

Communications Security (COMSEC)—(1) Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of communications security material. (2) The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study.

Communications Security (COMSEC) Account—Administrative entity, identified by an account number, used to maintain accountability, custody, and control of communications security material.

Communications Security—(COMSEC) Aid COMSEC material that assists in securing telecommunications and is required in the production, operation, or maintenance of COMSEC systems and their components. COMSEC keying material, call sign/ frequency systems, and supporting documentation, such as operating and maintenance manuals, are examples of COMSEC aids.

Communications Security (COMSEC) Boundary—Definable perimeter that encompasses all hardware, firmware, and software components performing critical COMSEC functions, such as key generation and key handling and storage.

Communications Security (COMSEC) Control Program—Computer instructions or routines that controlling or affect the externally performed functions of key generation, key distribution, message encryption and decryption, or authentication.

Communications Security (COMSEC) Custodian—Person designated by proper authority to be responsible for the receipt, transfer, accounting, safeguarding and destruction of COMSEC material assigned to a COMSEC account.

Communications Security (COMSEC) End Item—A final combination of equipment or component parts ready for its intended use in a COMSEC application.

Communications Security (COMSEC) Equipment—Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor and, subsequently, by reconverting such information to its original form for authorized recipients; also, equipment designed specifically to aid in, or as an essential element of, the conversion process. COMSEC equipment includes cryptoequipment, crypto ancillary equipment, crypto production equipment, and authentication equipment.

Communications Security (COMSEC) Facility—Physical space used for generating, storing, repairing, or using COMSEC material.

Communications Security (COMSEC) Incident Monitoring Activity—The office within an Air Force organization that maintains a record of COMSEC activity incidents caused by elements of that

organization and makes sure all actions required in connection with the incident are completed.

Communications Security (COMSEC) Incident—Unauthorized access or entry (or attempt) to an information system. It can include browsing; disruption or denial of service; alteration or destruction of input, processing, storage, or output of information; or changes to the system's hardware, firmware, or software characteristics with or without the user's knowledge, instruction, or intent.

Communications Security (COMSEC) Insecurity—COMSEC incident that has been investigated, evaluated, and determined to jeopardize the security of COMSEC material or the secure transmission of information.

Communications Security (COMSEC) Material Control System (CMCS)—Logistics and accounting system through which COMSEC material marked "CRYPTO" is distributed, controlled, and safeguarded. Included are the COMSEC central offices of record, cryptologistic depots, and COMSEC accounts. COMSEC material other than key may be handled through the COMSEC Material Control System.

Communications Security (COMSEC) Material—Item designed to secure or authenticate telecommunications. COMSEC material includes, but is not limited to: key, equipment, devices, documents, firmware or software that embodies or describes cryptographic logic and other items that perform COMSEC functions.

Communications Security (COMSEC) Module—Removable component that performs COMSEC functions in a telecommunications equipment or system.

Communications Security (COMSEC) Monitoring—Act of listening to, copying, or recording transmission of one's own official telecommunications to analyze the degree of security.

Communications Security (COMSEC) No-Lone Zone—Area, room, or space that, when manned, must be occupied by two or more appropriately cleared individuals who remain within sight of each other.

Communications Security (COMSEC) Operations—COMSEC operations include distributing, safeguarding, destroying, and accounting for all COMSEC material at all administrative and operational COMSEC accounts and all COMSEC user locations.

Communications Security (COMSEC) Profile—Statement of COMSEC measures and materials used to protect a given operation, system, or organization.

Communications Security (COMSEC) Responsible Officer (CRO)—Individual authorized by an organization to order COMSEC aids from the COMSEC account and who is responsible for their protection.

Communications Security (COMSEC) Survey—Organized collection of COMSEC and communications information relative to a given operation, system, or organization.

Communications Security (COMSEC) System Data—Information required by a COMSEC equipment or system to enable it to properly handle and control key.

Communications Security (COMSEC) Training—Teaching of skills relating to COMSEC accounting, use of COMSEC aids, or installation, use, maintenance, and repair of COMSEC equipment.

Communications Terminal—The terminus of a communications circuit at which data can be entered or received. The terminus can be located with the originator of the data or the ultimate addressee.

Compact Disk-Read-Only Memory (CD-ROM)—An optical device (disk) capable of containing large amounts of information as minuscule indentations on the surface of the disk that are read by an optical

laser device. CD-ROM disk standard storage is 683 Megabytes (MB); this standard has been established by the International Standards Organization. In actuality, a maximum of 735 MB of information can be stored on a compact disk.

Compander—Contraction of the terms *Compressor* and *Expander*. In high frequency radio communications, a device used on audio (speech) circuits to improve their quality by reducing the effects of noise present on the circuits.

Compartmentalization—A nonhierarchical grouping of sensitive information used to control access to data more finely than with hierarchical security classification alone. Compartmented information is usually identified by a codeword and level of classification.

Compartmented Mode—Information systems security mode of operation wherein each user with direct or indirect access to a system, its peripherals, remote terminals, or remote hosts has all of the following: (a) Valid security clearance for the most restricted information processed in the system. (b) Formal access approval and signed non-disclosure agreements for that information to which a user is to have access. (c) Valid need-to-know for information to which a user is to have access.

Compatibility—The capability of two or more items or components of equipment or material to exist or function in the same system or environment without mutual interference, defined over some range of functions of interest.

Complimentary Metal-Oxide Semiconductor (CMOS)—Special memory in a computer that stores information about the computer's configuration.

Component—(1) In communications-electronics, a subsystem, assembly, subassembly, or other major element of an end item which is essential to the operation of some larger assembly. It is an immediate subdivision of the assembly to which it belongs. (***NOTE:*** Proper usage of the term is dependent on the frame of reference.) (2) A military department or agency of the Department of Defense (DoD).

Composition—The use of phototypesetting or electronic character generating devices to set type and produce camera copy, negatives, plates, or images for printing and microform production. Composition equipment includes: (1) electronic composition devices and output equipment that produce proportionally spaced characters and spaces, multiple type faces, and variable type sizes; (2) systems that use digital computers to perform line justification, hyphenation, and page makeup; (3) Output systems that use cathode ray tubes to generate copies; (4) devices that emulate composition equipment and that are used primarily to produce copy that is printed or micropublished.

Compromise—In communications security, the disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

Compromising Emanations—Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by telecommunications or automated information system equipment.

Compromising Emanations—Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by communications and information system equipment. See TEMPEST.

Computer—An electronic device capable of accepting and processing information and supplying the results. It usually consists of input, output, storage, arithmetic, logic, and control units. Synonym:

Automated Information System (AIS).

Computer Abuse—Intentional or reckless misuse, alteration, disruption, or destruction of data/information processing resources.

Computer-Aided Design (CAD)—Sophisticated computer software used in the design any type of object on a video display tube. It may allow views in various dimensions. CAD is used to draft many kinds of designs, including paper forms, interactive data-entry screen forms, process flows, and manufactured items. A CAD system may analyze the drafted item for various properties, test its failure points, simulate its machining or use, or simply produce a graphic image for later display or print-out.

Computer-Based Security—Security for the communications and information system provided through the use of automated security features.

Computer Cryptography—Use of a crypto-algorithm program stored in software or firmware, by a general-purpose computer to authenticate or encrypt and/or decrypt data for storage or transmission.

Computer Emergency Response Team (CERT)—An organization chartered by an information system owner to coordinate and/or accomplish necessary actions in response to computer emergency incidents that threaten the availability or integrity of its information systems.

Computer Fraud—Computer-related crimes involving deliberate misrepresentation or alteration of data to get something of value, usually for monetary gain. A computer system must have been involved in the perpetration or cover-up of the act, or series of acts, through improper manipulation of input or output data, applications programs, data files, computer operations, communications, or computer hardware, software, or firmware.

Computer Graphics Metafile (CGM)—Standard for the description, storage, and communication of graphical information in a device-independent manner.

Computer Intrusion—An event of unauthorized entry, or attempted entry, to a computer system.

Computer Network—A computer network consists of computers and the communications components required to allow the exchange of information, files, sharing resources, etc.

Computer Network Attack (CNA)—Operations conducted via information systems to disrupt, deny, degrade, or destroy, information resident in computers and computer networks, or the computers and networks themselves.

Computer Network Defense (CND)—Those actions taken to plan, direct, and execute the response to unauthorized activity in defense of Air Force information systems and computer networks. Defense of the network includes a multilayered internal and external defense structure.

Computer Network Exploitation (CNE)—Intelligence collection operations that obtain information resident in files of threat automated information systems (AIS) and gain information about potential vulnerabilities, or access critical information resident with foreign AIS that could be used to the benefit of friendly operations.

Computer Output Microform (COM)—Microform produced directly from digital data.

Computer Program Configuration Item (CPCI)—An aggregate of computer program components, modules, routines, and so forth, which satisfy an end-use function and which is designated by the government for configuration management. CPCIs may vary widely in complexity, size, and type to form a special-purpose diagnostic program to a large command and control system. CPCIs represent a

requirement, of a set of requirements allocated from the functional baseline of a program/project.

Computer Program—An identifiable series of instructions or statements, in a form acceptable to a computer, prepared to achieve a certain result.

Computer Resources—(1) The totality of computer hardware, firmware, software, personnel, documentation, supplies, services, and support services applied to a given effort. (2) Components physically part of, dedicated to, or essential in real-time to mission performance; used for weapon system specialized training, simulation, diagnostic tests, maintenance, calibration, or research and development of weapon systems.

Computer Resources Life Cycle Management Plan (CRLCMP)—A program management document that describes the development, acquisition, test, and support plans over the life of the computer resources integral to, or used in, direct support of systems.

Computer Security (COMPUSEC)—The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems.

Computer Security Engineering Team (CSET)—Deployable Air Force Information Warfare Center teams that provide assistance to computer users and to Air Force organizations. The teams also provide assistance to control and recover from intrusion activity.

Computer Security Incident—See Incident.

Computer Security Policy—Set of laws, rules, and practices that regulate how an organization protects computer systems and the data within them.

Computer Security Subsystem—Hardware/software designed to provide computer security features in a larger system environment.

Computer Security Technical Vulnerability Reporting Program (CSTVRP)—Program that focuses on technical vulnerabilities in commercially available hardware, firmware, and software products acquired by DoD. Note: CSTVRP provides for reporting, cataloging, and discreet dissemination of technical vulnerability and corrective-measure information on a need-to-know basis.

Computer Software—A set of instructions, rules, routines, or statements that allow or cause a computer to perform a specific operation or series of operations; or source code listings, object codes, design details, algorithms, processes, flow charts, formulae, and related material that would enable the software to be created or recreated, compiled or recompiled, and produced or reproduced. The term does not include computer databases.

Computer Software Configuration Item (CSCI)—A computer program or group of related programs that satisfy an end use function and are set aside for separate configuration management.

Conditioned Circuit—A telecommunications circuit that has been optimized by means of conditioning equipment to obtain the desired characteristics for voice or data transmission.

Conditioning Equipment—Corrective networks used to equalize the insertion loss versus frequency characteristics and the envelope delay distortion over a desired frequency range of a circuit or line in order to obtain the desired quality of voice or data signals. Also, at junctions of circuits, equipment used to match transmission levels and impedances and to provide equalization between facilities.

Cone of Silence—In an omni-directional antenna, transmitting in a horizontal plane, the radiation pattern is such that there is an area directly above the antenna in which there is no radiated energy. This area is

roughly in the shape of an inverted cone, hence the name. This phenomena is used by airplanes to determine their position over or near a given location.

Conference for Data System Languages (CODASYL)—A group created by DoD that includes users and manufacturers, and considers the development of COBOL and hardware-independent software for database management.

Confidentiality—Assurance that information is not disclosed to unauthorized persons, processes, or devices.

Configuration—A collection of an item's descriptive and governing characteristics which can be expressed in functional terms (what performance the item is expected to achieve) and physical terms (what the item should look like and consist of).

Configuration Audits—The verification of the configuration item's conformance to specifications and other contract requirements.

Configuration Control—Process of controlling modifications to hardware, firmware, software, and documentation to ensure the communications system is protected against improper modifications.

Configuration Item (CI)—(1) A collection of an item's descriptive and governing characteristics which can be expressed in functional terms, i.e., what performance the item is expected to achieve, and in physical terms, i.e., what the item should look like and consist of when it is built. (2) An aggregation of hardware, firmware, or computer software or any of its discrete portions, which satisfies an end-use function and is designated by the government for separate configuration management. A CI may vary widely in complexity, size, type, from an aircraft, ship, or electronic system to a test meter or round of ammunition. Any item required for logistics support and designed for separate procurement is a configuration item.

Configuration Management (CM)—(1) A discipline applying technical and administrative surveillance to: (a) identify and document the functional and physical characteristics of a configuration item; (b) control changes to those characteristics; and (c) record and report changes to processing and implementation status. (2) Technical and organizational activities comprising configuration identification, configuration control, configuration status accounting, and configuration auditing.

Conical Antenna—An antenna consisting of two conically-shaped conductors or elements, having a common axis and vertex, and extending in opposite directions.

Constant False Alarm Rate (CFAR)—In radar, a receiver technique that varies the detection threshold level (sensitivity) with the noise or clutter level to maintain a constant false alarm probability. Also called False Alarm Rate (FAR).

Consulting Committee on International Telephone and Telegraph (CCITT)—An international committee operating under the auspices of the International Telecommunications Union. The committee makes recommendations on the relevant characteristics of the respective national telecommunications systems that may form part of the international connections.

Contamination—In information assurance, (a) the introduction of data of one security classification or security category into data of a lower security classification or different security category, and (b) intermixing of data at different sensitivity and need-to-know levels. The lower level data is said to be contaminated by the higher level data; thus, the contaminating (higher level) data may not receive the required level of protection.

Content Management—In the context of the Air Force Portal, the process of validating information requirements and identifying, organizing, and approving data and information systems to be accessed through the Air Force portal. In the context of Air Force enterprise information resources, the process of building, assessing the overall adequacy of, and maintaining the information capabilities needed to support Air Force business and combat operations.

Content Manager—In the context of the Air Force portal, the individual within a functinal area, MAJCOM, or at the Headquarters USAF level, who validates information requirements, reviews proposed information systems to identify candidates to bring onto the Air Force portal, adds, removes, and modifies content, monitors quality, and assists the Air Force CIO development of user handbooks, develops guides, templates and content checklists. Content managers facilitate the interactions between content providers and Air Force portal service providers.

Contingency Key—Key held for use under specific operational conditions or in support of specific contingency plans.

Continuously Variable Slope Delta (CVSD)—In telecommunications, an analog to digital conversion based on delta modulation. Widely used in joint tactical communications equipment.

Contractor Logistics Support (CLS)—A preplanned method used to provide all or part of the logistics support to a new system/equipment or modification, throughout its entire life cycle, by a contractor.

Control—In communications security, prescribed actions taken to maintain the appropriate level-of-protection for communications and information systems. Controls may validate security activities, detect security incidents and non-conformance, correct deficient security countermeasures, measure the assurance of communications and information system activities, or report incidents.

Controlled Access Protection (CAP) Administrator—Individual responsible for granting and withdrawing cryptographic access within a unit or organization.

Controlled Area—Any building, area, or structure containing Air Force resources that are a lucrative target for theft, compromise, or destruction and to which entry must be limited to provide more protection.

Controlled Cryptographic Item (CCI)—Secure telecommunications or information handling equipment, or associated cryptographic component, that is unclassified but governed by a special set of control requirements.

Controlled Cryptographic Item (CCI) Assembly—Device embodying a cryptographic logic or other COMSEC design that the National Security Agency has approved as a CCI and performs the entire COMSEC function, but is dependent upon the host equipment to operate.

Controlled Cryptographic Item (CCI) Component—Device embodying a cryptographic logic or other COMSEC design, that the National Security Agency has approved as a CCI, that does not perform the entire COMSEC function and is dependent upon the host equipment or assembly to complete and operate the COMSEC function.

Controlled Cryptographic Item (CCI) Equipment—Telecommunications or information handling equipment that embodies a Controlled Cryptographic Item component or assembly and performs the entire communications security function without dependence on host equipment to operate.

Controlled Space—Three-dimensional space surrounding communications and information system equipment, within which unauthorized persons are denied unrestricted access and are either escorted by authorized persons or are under continuous physical or electronic surveillance.

Controlling Authority—Official responsible for directing the operation of a cryptonet and for managing the operational use and control of keying material assigned to the cryptonet.

Cookie—On the Internet, a message from a Web browser to a Web server. The browser stores the message on the user's PC in a text file called cookie.txt. The message is sent back to the server each time the browser requests a page from the server. The server can use this information to present the user with customized Web pages.

Cooperative Key Generation (CKG)—Electronically exchanged functions of locally generated, random components, from which both terminals of a secure circuit construct traffic encryption key or key encryption key for use on that circuit.

Corrective Maintenance—All unscheduled maintenance actions performed as a result of a system failure and that are required to restore the system to a specified condition. Also called unscheduled maintenance.

Counterinformation (CI) Operations—Actions that seek to establish a desired degree of control in information functions that permit friendly forces to operate at a given time or place without prohibitive interference by the opposing force.

Countermeasure (CM)—(1) Any action, device, procedure, technique, or other measure that reduces the vulnerability of an Information System; also called a safeguard. A countermeasure protects against a specific threat type or mechanism. (2) The sum of a safeguard and its associated controls.

Countermeasures Review—A technical evaluation of a facility to identify the inspectable space, the required countermeasures, and the most cost effective way to apply required countermeasures.

Covert Channel Analysis—Determination of the extent to which the security policy model and subsequent lower-level program descriptions may allow unauthorized access to information.

Covert Channel—An unintended and/or unauthorized communications path that can be used to transfer information in a manner that violates a system's security policy.

Covert Storage Channel—Covert channel involving the direct or indirect writing to a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a finite resource (e.g., sectors on a disk) that is shared by two subjects at different security levels.

Covert Timing Channel—Covert channel in which one process signals information to another process by modulating its own use of system resources (e.g., central processing unit time) in such a way that this manipulation affects the real response time observed by the second process.

Cracker—A person who attempts to gain access to computers for which he or she does not have authorization.

Credentials—In communications security, information passed from one entity to another, which is used to establish the sending entity's access rights.

Critical Asset—Any facility, equipment, service or resource considered essential to DoD operations in peace, crisis, and war and warranting measures and precautions to ensure its continued efficient operation, protection from disruption, degradation or destruction, and timely restoration. Critical assets may be DoD assets or other government or private assets (e.g., industrial or infrastructure critical assets), domestic or foreign, whose disruption or loss would render DoD critical assets ineffective or otherwise seriously

disrupt DoD operations.

Critical Information (CI)—Information about friendly (US, allied and coalition) activities, intentions, capabilities, or limitations, that an adversary needs in order to gain a military, political, diplomatic or technological advantage. Such information, if released prematurely, may prevent or forestall mission accomplishment, reduce mission effectiveness, or cause loss of lives or damage to friendly resources.

Critical Infrastructures—National infrastructures whose incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and distribution, banking and finance, transportation, water supply systems, emergency services, and continuity of government.

Critical Processing—Processing that must continue in a correct and uninterrupted manner to support DoD emergency or war plans, preserve human life or safety, or support the mission of the using organization.

Critical Program Information—Technologies, programs, or systems that, if compromised, would degrade combat effectiveness, shorten the expected combat-effective life of the system, or significantly alter program direction. This includes classified military information or unclassified controlled information about such programs, technologies, or systems.

Critical Technical Load—That part of the total technical electrical power required to operate the synchronous communications and automatic switching equipment in a communications facility.

Criticality—Computer security characteristic that measures how important the correct and uninterrupted functioning of the communications and information system is to national security, human life or safety, or the mission of the using organization.

Crosslink—In satellite communications, the direct transmission link between two orbiting satellites.

Cross-Polarization—In radio communications, refers to the polarization of the transmit and receive antennas of a radio link or system. Cross-polarization is a method to improve performance of the radio link by reducing or counteracting the effects of fading of the radio signals. It involves the use of two transmitters operating on the same frequency, with one transmitter-receiver pair being vertically polarized, and the other pair horizontally polarized.

Crosstalk—(1) The condition in which a signal transmitted on one circuit or channel of a transmission system is detectable in another circuit or channel. (2) Unwanted transfer of energy from one communications channel to another.

Cryptanalysis—Operations performed in converting encrypted messages to plain text without initial knowledge of the crypto-algorithm and/or key employed in the encryption.

Crypto—Marking or designator identifying communications security keying material used to secure or authenticate telecommunications carrying classified or sensitive U.S. Government or U.S. Government-derived information.

Crypto-Alarm—Circuit or device that detects failures or aberrations in the logic or operation of cryptoequipment. Crypto-alarm may inhibit transmission or may provide a visible and/or audible alarm.

Crypto-Algorithm—Well-defined procedure or sequence of rules or steps, or a series of mathematical equations used to describe cryptographic processes such as encryption/decryption, key generation, authentication, signatures, etc.

Crypto-Ancillary Equipment—Equipment designed specifically to facilitate efficient or reliable operation of cryptoequipment, without performing cryptographic functions itself.

Crypto-Channel—A complete system of crypto-communications between two or more holders. The basic unit for naval cryptographic communication. It includes: (a) the cryptographic aids prescribed; (b) the holders thereof; (c) the indicators or other means of identification; (d) the area or areas in which effective; (e) the special purpose, if any, for which provided; and (f) pertinent notes as to distribution, usage, etc. A crypto-channel is analogous to a radio circuit.

Cryptoequipment—Equipment that embodies a cryptographic logic.

Cryptographic Access Program (CAP)—A program to protect national security information and to govern access to cryptographic information that the DoD produces, controls, or owns.

Cryptographic Component—Hardware or firmware embodiment of the cryptographic logic. Cryptographic component may be a modular assembly, a printed wiring assembly, a microcircuit, or a combination of these items.

Cryptographic Information—All information significantly descriptive of cryptographic techniques and processes or of cryptographic systems and equipment, or their functions and capabilities, and all cryptomaterial.

Cryptographic Initialization—Function used to set the state of a cryptographic logic prior to key generation, encryption, or other operating mode**.**

Cryptographic Logic—The embodiment of one or more crypto-algorithms along with alarms, checks, and other processes essential to effective and secure performance of the cryptographic process.

Cryptographic Randomization—Function that randomly determines the transmit state of a cryptographic logic**.**

Cryptography—Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form**.**

Crypto-Ignition Key (CIK)—Device or electronic key used to unlock the secure mode of cryptoequipment.

Cryptomaterial—All material, including documents, devices, equipment, and apparatus, essential to the encryption, decryption, or authentication of telecommunications. When classified, it is designated CRYPTO and subject to special safeguards.

Cryptonet—Stations holding a common key.

Cryptopart—A division of a message as prescribed for security reasons. The operating instructions for certain cryptosystems prescribe the number of groups which may be encrypted in the systems, using a single message indicator. Cryptoparts are identified in plain language. They are not to be confused with message parts.

Cryptoperiod—Time span during which each key setting remains in effect.

Cryptosecurity—Component of COMSEC resulting from the provision of technically sound cryptosystems and their proper use.

Cryptosynchronization—Process by which a receiving decrypting cryptographic logic attains the same internal state as the transmitting encrypting logic.

Cryptosystem—Associated information systems security items interacting to provide a single means of encryption or decryption.

Cryptonet Member—An individual station, among a group of stations, holding a specific key for use. Controlling authorities are defacto cryptonet members.

Cursor—Visual mechanism to mark, on-screen, where current input or output is to happen.

Cyberspace—(1) The term that describes the whole range of information resources available through computer networks, the internet, and connected on-line services. (2) The realm of digitized information accessible through electronic communications that exists within computers and the telecommunications networks that connect them. (The term was originated by author William Gibson in his novel *Neuromancer.*)

Cyclic Redundancy Check—Error checking mechanism that checks data integrity by computing a polynomial algorithm based checksum.

Dangling Threat—In communications security, a set of properties about the external environment for which there is no corresponding vulnerability and therefore no implied risk.

Dangling Vulnerability—In communications security, a set of properties about the internal environment for which there is no corresponding threat and therefore no implied risk.

Data—(1) A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations, such as characters or analog quantities, to which meaning is or might be assigned. (2) A general term used to denote any or all facts, numbers, letters, and symbols that refer or describe an object, idea, condition, situation, or other factor.

Data Administrator—A person or group that ensures the utility of data used within an organization by defining data policies and standards, planning for the efficient use of data, coordinating data structures among organizational components, performing logical database designs, and defining data security procedures.

Data Aggregation—(1) The compilation of unclassified individual data systems and data elements resulting in the totality of the information being classified. **(**2) Data aggregation is the convergence of information. This becomes a problem when certain information or data elements at one sensitivity level requires reclassification at a higher level when combined or associated with other information. Aggregate data would require classification if the new information meets the specific classifying criteria as defined in DoD 5200.1-R or reclassification according to classification guidance provided by the functional OPR.

Data Architecture—A framework for organizing data into a manageable grouping to facilitate shared use and control throughout the Air Force.

Data Attribute—A characteristic of a unit of data such as length, value, or method of representation.

Data Bank—A comprehensive collection of data which may be structured as follows: one line of an invoice may form an item; a complete invoice may form a record; a complete set of such records may form a file; and the collection of files used by an organization may be known as its data bank.

Data Code—A number, letter, character, or any combination thereof used to represent a data element or data item. For example, the data codes E8, 03, and 06 might be used to represent the data items of sergeant, captain, and colonel under the data element military personnel grade.

Data Communications Protocol Standards (DCPS)—A standardization area of the Defense Standardization Program. This area establishes DoD protocol standards and reference protocol architectures necessary to support Intranet work host-to-host data communications using digital communications techniques. The DCPS area involves standardization of Internet work, peer, and interlayer management protocols, including those that deal with end-to-end (host-to-host) communications across a network or a concatenated set of networks.

Data Compression—The process of reducing bandwidth, cost, and time for the generation, transmission, storage of data by employing techniques designed to remove data redundancy. Data compression standards specify algorithms for compressing data for exchange over a network; it can reduce communications loading by as much as 80 percent without affecting the form of transmitted data.

Data Concentrator—A functional unit that permits a common transmission medium to serve more data sources than there are channels available within the transmission medium.

Data Contamination—Deliberate or accidental process or act resulting in a change in the integrity of the original data.

Data Dictionary/Directory Services—Key computer software tools that manage data and information resources. Such services provide extensive facilities for recording, storing, and processing descriptions of an organization's significant data and data processing resources, and often provide facilities to use metadata (information about data).

Data Dictionary—A specialized type of database containing metadata, and managed by a data dictionary system; a repository of information describing the characteristics of data used to design, monitor, document, protect, and control data in information systems and databases; an application of a data dictionary system.

Data Element—A basic unit of information built on standard structures having a unique meaning and distinct units or values. Examples of data elements are: rank, grade, age, etc.

Data Encryption Standard (DES)—Cryptographic algorithm, designed for the protection of unclassified data and published by the National Institute of Standards and Technology in Federal Information Processing Standard Publication 46.

Data Field—The defined area, usually a column or columns, on a numbered line or block, where a data element is entered.

Data File—Related numeric, text, or graphic information that is organized in a strictly prescribed form and format.

Data Flow Control—Synonymous with information flow control.

Data Fusion—In command and control (C2) operations, the bringing together of fusing of independently obtained data to obtain a bigger picture of the whole (for example, data obtained from sensors that are significantly different, such as a video image being fused with information from a radio transmission.)

Data Integrity—(1) A property of data in which all assertions (accurate, current, consistent, complete) hold. (2) The assurance that the data received is the same data as the data that was sent. (3) The concept that the database management system will perform its function consistently, preserve data without unintentional change, produce correct results to the defined degree of precision, and maintain data availability.

Data Interchange Standards Association (DISA)—A non-profit organization that administers the X.12 standard for the ANSI X.12 subcommittee and provides news updates on electronic data interchange.

Data Item—A subunit of descriptive information or value classified under a data element. For example, the data element “military personnel grade” contains data items such as sergeant or captain.

Data Management—The function of controlling the acquisition, analysis, storage, retrieval, and distribution of data.

Data Origin Authentication—Corroboration that the source of data is as claimed.

Data Processing—(1) Any procedure for receiving information and producing a specific result. (2) Executing sequences of operations on data, such as merging, sorting, calculating, and printing.

Data Repository—A repository provides a place and method to store metadata. It generally is broader and supports more kinds of data than a data dictionary.

Data Resource—Any data created manually or by automatic means and used by a system or enterprise to represent its information.

Data Security—Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.

Data Sensitivity—The identification of how important the data processed by the system is and the extent of the protection that must therefore be provided to the system and its data.

Data Server—The data server provides data services to clients. A client will send a request to a data server (sometimes called a “database server”) and the server will respond with the results of the request. The accessing and updating of the data maintained on the data server is performed by the data server, not by the clients. It supports the implementation of better controls by managing access to the data resident within the server. The data server can also be optimized to the type of data it is being asked to manage; a data server could support archiving and be based on optical storage technology rather than magnetic.

Data Sink—A device that receives data signals from a data source.

Data Steward—A person or group that manages the development, approval, and use of data within a specified functional area, ensuring that it can be used to satisfy data requirements throughout the organization.

Data Stewardship—The concept that emphasized the role of content providers and content managers in providing information capabilities to the Air Force enterprise to be shared with other users. It contrasts with the concept of data ownership where a content provider or content manager would control access to "their" information resources.

Data Structure—The framework that defines the specifics about one or more types of data that support the user system. The data structure includes the collection of record types, linkages, fields, entry points, and integrity rules.

Data Systems Authorization Directory (DSAD)—The official HQ USAF-approved directory of data system descriptions with assigned data system designators and authorized for processing by Air Force activities. It is an inventory of authorized data systems and reflects Air Force activities authorized to process individual applications and the specific types of automated data processing equipment on which the applications are processed. System descriptions contained in the DSAD may be for systems under development or in operation. The status of an individual system can be determined by the implementation

schedule or the activities responsible for the design, implementation, and maintenance. The DSAD is published by the Standard Systems Group.

Data Terminal Equipment (DTE)—Equipment consisting of digital-end instruments that convert the user information into data signals for transmission or reconvert the received data signals into user information. The functional unit of a data station that serves as a data source of a data link and provides for the data communication control function to be performed in accordance with link protocol. The DTE may consist of a single piece of equipment that provides all the required functions necessary to permit the user to intercommunicate, or it may be an interconnected subsystem of multiple pieces of equipment, to perform all the required functions.

Data Transfer Device (DTD)—Fill device designed to securely store, transport, and transfer electronically both communications security and transmission security key, designed to be backwards compatible with the previous generation of communications security common fill devices, and programmable to support modern mission systems.

Data Transfer Rate—A particular rate at which data is transmitted through a channel but measured during the time the data is actually being transmitted.

Data Warehouse—A database designed to support decision making in an organization or enterprise and that is capable of containing enormous amounts of data.

Database—(1) Information that is normally structured and indexed for user access and review. Databases may exist in the form of physical files (folders, documents, and so forth) or formatted automated data processing system data files. (2) A structured or organized collection of information, which may be accessed and manipulated by the computer. (3) A set of data that is required for a specific purpose that is fundamental to a system, project, enterprise, or business. A database may consist of one or more data banks and be geographically distributed among several repositories. Databases may exist in the form of physical files or formatted automated data processing system data files.

Database Administration—(1) The analysis, classification, and maintenance of an organization's data and data relationships. It includes the development of data models and dictionaries, which combined with transaction processing, are the raw materials for database design. It includes the development of data models and dictionaries, which combined with transaction processing, are the raw materials for database design. (2) The activity responsible for enforcing policies and standards set by the database administrator, to include providing technical support for physical database definition, design, implementation, maintenance, integrity, and security, and coordinating with computer operations technicians, system developers, vendors, and users.

Debug—In computing, the process to locate and correct errors in a computer program.

Deca (da)—A prefix denoting ten (10^{+1}).

Decertification—Revocation of the certification of an information system item or equipment for cause.

Decibel (dB)—In communications-electronics, the standard unit for expressing transmission or signal gain or loss and relative power ratios. The decibel is one-tenth of a bel, which is too large a unit for convenient use. Both units are expressed in terms of the logarithm to the base 10 of the ratio of two levels of power.

Decipher—Convert enciphered text to plain text by means of a cryptographic system.

Declassification—The determination that in the interests of national security, classified information no

longer requires any degree of protection against unauthorized disclosure, coupled with removal or cancellation of the classification designation.

Declassification (Of Magnetic Storage Media)—Administrative decision or procedure to remove or reduce the security classification of the subject media.

Declassify—To cancel the security classification of an item of classified matter. See also downgrade.

Decode—Convert encoded text to plain text by means of a code.

Decrypt—(1) Generic term encompassing decode and decipher. (2) To convert encrypted text into its equivalent plain text by means of a cryptosystem. This does not include solution by cryptanalysis.

Decryption—The restoration of encrypted data to its original plain text or other readily usable state.

Dedicated Mode—Information system security mode of operation wherein each user, with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has all of the following: (a) Valid security clearance for all information within the system. (b) Formal access approval and signed non-disclosure agreements for all the information stored and/or processed (including all compartments, subcompartments, and/or special access programs). (c) Valid need-to-know for all information contained within the Information System. When in the dedicated security mode, a system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time.

Dedicated Server—A computer (or node) on which applications are limited to maintaining network resources. No user applications are available.

Dedicated Systems—Information processing components devoted to satisfying a unique mission or functional information need beyond the capability of shared systems; functional end-user organizations generally control these resources.

Default Classification—Temporary classification reflecting the highest classification being processed in an Information System. Default classification is included in the caution statement affixed to an object.

Defense Automated Visual Information System (DAVIS)—A standard DoD-wide automated data processing system for visual information (VI) management purposes at DoD component and major command levels. It includes a production database covering production, acquisition, inventory, distribution, product status, and archival control of audiovisual productions and VI materials, and VI facilities' database that includes activities, facilities, personnel, and funds.

Defense Commercial Telecommunications Network (DCTN)—A leased communications system that provides common user switched voice, dedicated voice and data, and video teleconferencing services throughout the United States. This fully integrated digital network uses satellite and terrestrial transmission to serve U.S. Government installations nationwide. The DCTN interfaces with the Defense Switched Network and the Federal Telephone System 2000.

Defense Information Infrastructure (DII)—The DII is the web of communications networks, computers, software, databases, applications, and other services that meet the information processing and transport needs of DoD users, across the range of military operations. The DII includes the information infrastructure of the Office of the Secretary of Defense, the military departments, the Chairman of the Joint Chiefs of Staff, the Defense agencies, and the combatant commands. It provides information processing and services to subscribers over the Defense Information System Network and includes command and control, tactical, intelligence, and commercial communications systems used to transmit

DoD information. The DII is embedded within and deeply integrated into the National Information Infrastructure. Their seamless relationship makes distinguishing between them difficult.

Defense Information Infrastructure/Common Operating Environment (DII/COE)—(1) The DII/COE concept emphasizes both software reuse and interoperability; however, it is much broader in scope than simple software reuse. The DII/COE is not a system; it provides a foundation for building open systems. It is a "plug-and-play" open architecture designed around a client/server model; it offers a collection of services and already built modules for mission application. The DII/COE is also an evolutionary acquisition and implementation strategy. It emphasizes incremental development and fielding to reduce the time required to put a new functionality into the hands of the user. (2) The DII/COE establishes an integrated software infrastructure which facilitates the migration and implementation of functional mission applications and integrated databases across information systems in the DII. The DII/COE provides architecture principles, guidelines, and methodologies that assist in the development of mission application software by capitalizing on a thorough, cohesive, set of infrastructure support services.

Defense Information Operations (DIO)—The DIO process integrates and coordinates policies and procedures, operations, personnel, and technology to protect information and to defend information systems. DIOs are conducted through information assurance, physical security, operations security, counter deception, counter psychological operations, counter intelligence, electronic protect, and special information operations.

Defense Information Systems Agency (DISA)—A U.S. Government agency with the mission to exercise operational direction and management control of the Defense Information System to meet the long haul, point-to-point, and switched network telecommunications requirements of the National Command Authorities, DoD, and other U.S. Government agencies as authorized and directed by the Secretary of Defense.

Defense Information Systems Agency Information Network (DISANET)—DISANET is DISA's consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting DISA's operations. It is transparent to its users, facilitates the management of information resources, and is responsive to DISA's missions and needs. DISANET is a sub-element of the DISA Information System,

Defense Information Systems Network (DISN)—An enhanced long-haul telecommunications infrastructure that supports a full range of communications services (voice, data, and video) for DoD activities worldwide. It is the DoD's worldwide enterprise-level telecommunications infrastructure that provides end-to-end information transfer for supporting military operations. It is transparent to its users, facilitates the management of information resources, and is responsive to national security and defense needs. The DISN is an element of the Global Information Grid (GIG).

Defense Message System (DMS)—DMS is a flexible, secure, commercial-off-the-shelf (COTS) based system providing multi-media messaging and directory services taking advantage of the underlying Defense Information Infrastructure network and services.

Defense Printing Service (DPS)—The service that manages the DoD consolidated printing and duplicating organizations. The DPS is a subordinate unit of the United States Navy, who is the executive agent for DoD printing.

Defense Red Switch Network (DRSN)—A network of the Defense Information System Network consisting of a global secure voice switching network whose subscribers are served by a variety of

automatic switches and manual operator switchboards. All switchboards are interconnected within the network by dedicated wideband trunk circuits and/or narrowband Defense Switched Network.

Defense Satellite Communications System (DSCS)—The worldwide military satellite network managed by the Defense Information Systems Agency, comprising orbiting space segments and ground terminals and control segments that operate in the super-high frequency band to provide long-haul multi-channel communications connectivity.

Defense Switched Network (DSN)—The DSN is the switched circuit telecommunications system of the Defense Information System Network (DISN). It provides end-to-end common-user and dedicated telephone service, voice-band data, and video teleconferencing for the DoD. The DSN provides rapid and low-cost long haul, secure and non-secure voice, data, and video services throughout the DoD.

Defense-Wide Information Assurance Program (DIAP)—An overarching DoD-level program established by the Deputy Secretary of Defense to ensure the protection and reliability of the Defense Information Infrastructure. The DIAP implements a DoD-wide Information Assurance planning and integration framework. It infuses Information Assurance throughout DoD operations as a fundamental element of readiness and training.

Defensive Counterinformation (DCI)—Activities which are conducted to protect and defend friendly information and information systems.

Defensive Information Operations (DIO)—The integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend information and information systems. DIOs are conducted through information assurance, physical security, operations security, counter-deception, counter-psychological operations, counterintelligence, electronic warfare, and special information operations. DIOs ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes.

Degausser—Electrical device or hand held permanent magnet that can generate a high intensive magnetic field to purge magnetic storage media.

Degausser Products List (DPL)—List of commercially produced degaussers that meet National Security Agency specifications. This list is included in the National Security Agency Information Systems Security Products and Services Catalogue, and is available through the Government Printing Office.

Degaussing—The neutralization or removal of the magnetization of a mass of magnetic material. Degaussing renders any stored data on magnetic media unreadable and is used in the sanitizing of magnetic storage tapes, and computer disks and diskettes. Also called demagnetizing.

Degrees Of Assurance—Measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy. The degrees of assurance (i.e., low, medium, and high) for availability, integrity, confidentiality, and authenticity are directly related to the expected consequences resulting from loss of systems or information.

Delay Equalizer—An electronic device designed to make the phase or envelope delay of a circuit or system substantially constant over a desired frequency range.

Delay Line—A real or artificial transmission line or equivalent device designed to introduce specific time delays to the signals passing through the line.

Delegated Development Program—Information security program in which the director, National Security Agency, delegates, on a case by case basis, the development and/or production of an entire telecommunications product, including the information systems security portion, to a lead department or agency.

Delta Modulation—In telecommunications, a modulation technique for converting an analog signal to a digital signal.

Demand Assignment—In satellite communications, an operational technique where various users share a satellite capacity on a real-time demand basis. A user needing to communicate with another user of the network activates the required circuit; upon completion of the communication, the circuit is deactivated and the satellite capacity is made available for other users.

Demodulation—The reverse of modulation. A technique where the modulated (typically radio frequency) signal is processed (demodulated) to retrieve the original modulating (i.e., input/intelligence) signal.

Demultiplex—The reverse of multiplex. Compare modulation and demodulation.

Denial Authority—Individuals with authority to deny requests for access or amendment of records under the Privacy Act and the Freedom of Information Act.

Denial of Service—Result of any action or series of actions that prevents any part of a communications and information system from functioning.

Department of Defense Directive (DODD)—A broad DoD policy document containing what is required by legislation, the President, or the Secretary of Defense to initiate, govern, or regulate actions or conduct by DoD components within their specified areas of responsibilities. DODDs establish or describe policies, programs; and organizations; define missions; establish organizations; provide authority; and assign responsibilities.

Department of Defense Directives System Transmittals—The notice that changes or cancels a DoD directive, DoD instruction, or DoD publication.

Department of Defense Directive-Type Memorandum—A memorandum issued by the Secretary of Defense, Deputy Secretary of Defense, or Office of the Secretary of Defense Principal Staff Assistants (PSA) that, because of time constraints, cannot be published in the DoD Directives System. Directive-type memorandums signed by PSAs are procedural in nature. They implement policy documents, such as DoD directives, Federal laws, and Executive Orders. Directive-type memorandums signed by the Secretary or Deputy Secretary of Defense are policy-making documents.

Departmental Printing—Printing (such as publications, forms, and visual aids) used throughout the Air Force, regardless of origin. AFDPO/PP buys departmental printing through the Defense Printing Service and the Government Printing Office.

Design Controlled Spare Part—Part or subassembly for a communications security item of equipment or device with a National Security Agency controlled design.

Design Documentation—Set of documents, required for Trusted Computer System Evaluation Criteria (TCSEC) classes C1 and above (as defined in the Orange Book, Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD), whose primary purpose is to define and describe the properties of a system. As it relates to TCSEC, design documentation provides an explanation of how the security policy of a system is translated into a technical solution via the Trusted

Computer Base hardware, software, and firmware.

Designated Approving Authority (DAA)—Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Accrediting Authority, Delegated Accrediting Authority, and Communications And Information Systems Security Manager.

Desktop Publishing—Software programs using a microcomputer (and usually a component of an office automation system) to electronically arrange text and graphics as composition. Output is then produced on an electronic laser printer, ink jet printer, or similar output device in a page format. The output may be reproduced using printing methods.

Dial Central Office (DCO)—A private telephone exchange/switch that usually includes access to the public switched network, which provides dial service on subscribers' premises and serves only their stations with local and trunked communications.

Dibit—A group of two bits. The four possible states for a dibit are 00, 01, 10, and 11.

Dichroic Filter—An optical filter that reflects one or more optical bands or wavelengths and transmits others, while maintaining a nearly zero coefficient of absorption for all wavelengths of interest. A dichroic filter may be high-pass, low-pass, band-pass, or band rejection.

Differential Phase Shift Keying (DPSK)—A method of modulation employed for digital transmission. In DPSK each signal element is a change in the phase of the carrier with respect to its previous phase angle.

Diffraction—The natural phenomenon of the bending of a radio or light wave around the edge of an object, barrier, or aperture. In radio communications, this allows radio waves to penetrate into what normally would be a shadow region behind the object, such as a mountain peak. Also referred to as the knife-edge effect.

Digital Certificate—An electronic "credit card" that establishes the user's credentials when conducting business or other transactions on the Internet. It is issued by a Public Key Infrastructure certification authority.

Digital Channel—A means for conveying information in digital form from one point to another.

Digital Circuit—A combination of two digital channels permitting bi-directional digital transmissions between two points, to support a single communication.

Digital Data Service (DDS)—A generic description for synchronous digital transmissions operating at a rate of up to 64 kb/s.

Digital Distribution Unit (DDU)—A device designed to take a digital input and transmit the signal in a quasi-analog form over a voice grade telephone line and vice versa. The most popular version uses a differential diphase modulation scheme that combines timing and data into one composite signal.

Digital Multiplexer—An item of communications equipment, part of a telecommunications system, that converts multiple audio signals (voice frequency channels) into an aggregate digital bit stream for transmission over a wideband radio system - and vice versa.

Digital Patch and Access System (DPAS)—A semi-automated patch and access system to provide the Defense Information System with the means to rapidly reconfigure digital circuits. The cross-connect capability of a DPAS permits the assignment and redistribution of channels on T1 carriers (DS-1 rate

1.544 Mbps) which use digital transmission systems.

Digital Signal (DS)—In telecommunications, a classification of digital circuits. Technically, DS refers to the rate and format of the signal, while the T (-carrier) designation refers to the equipment providing the signals. In the North American digital hierarchy, DS and T are used synonymously, e.g., DS1 and T1. (DS0 = 64 kbps; DS1 = 1.544 Mbps; DS2 = 6.312 Mbps; DS3 = 44.736 Mbps; DS4 = 274.176 Mbps; DS5 = 400.352 Mbps).

Digital Signature—(1) A transformation of a message or document using an asymmetric cryptosystem and a hash function such that a person having the initial message or document and a signer's public key can accurately determine the authenticity of the transformation. Digital signatures are a subset of electronic signatures; electronic signatures may or may not be linked to a document; digital signatures are inextricably linked to the document. (2) A method of ensuring that a message was sent by the person claiming to send it. The signature is encrypted with the sender's private key and decrypted by the recipient using the sender's public key.

Digital Signature Algorithm—Procedure that appends data to, or performs a cryptographic transformation of, a data unit. The appended data or cryptographic transformation allows reception of the data unit and protects against forgery, e.g., by the recipient.

Digital Signature Standard (DSS)—A cryptographic technique for authenticating electronic communications conforming to IEC 9796 International Digital Signature Standard and developed by the National Security Agency.

Digital Subscriber Line (DSL)—A method for moving data over regular telephone lines. A DSL circuit is much faster than a regular telephone connection. A DSL circuit must be configured to connect two specific locations, similar to a leased circuit.

Digital Video Disk (DVD)—A storage format that can store 4.5 GB of data on a disk that resembles a compact disk.

Digitize—To convert an analog signal to a digital signal.

Digroup—Abbreviation for "digital group." A term designating the basic digital multiplexing grouping. In the United States, this basic group is derived from 1.544 Mbps; in Europe, the basic group is commonly 2.048 Mbps.

Diplex Operation—Simultaneous one-way transmission or reception of two independent signals using a common element, such as an antenna system or a communications channel.

Diplexer—In radio communications systems, a multi-port coupling device which permits two transmitters or receivers to operate simultaneously without interaction using the same antenna system.

Direct Broadcast Satellite (DBS)—A new, high-powered, national satellite distribution system for video, audio, and data. The system consists of approximately 150 channels of standard resolution television that offers both standard 4:3 and wide screen 16:9 aspect ratios. DBS has potential for the Air Force and DoD to broadcast high volumes of information at speeds in the multi-megabit range to a wide variety of users throughout a theater of operations.

Direct Current (DC) Erasure—Degaussing with a hand-held permanent magnet or with DC electrical-powered equipment to saturate the media so the noise level is raised to mask the signal level. There should be no signal level detectable above the noise level after DC erasure.

Direct Data Exchange (DDE)—In data communications, the exchange of data between programs. Any changes made to the data in the source (server) application will automatically and dynamically be changed also in the current (client or receiving) application. The data in the current (client or receiving) program is said to be linked to that program.

Direct Memory Access (DMA)—In memory systems, a technique that allows a peripheral device to gain direct access to the main memory of the computer. When the peripheral initiates DMA the processor is compelled to stop all bus activity while the peripheral occupies the bus.

Directed Energy—An umbrella term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or subatomic particles.

Directive Publication—A publication that is necessary to meet the requirements of law, safety, security, or other areas where common direction and standardization benefit the Air Force. The language used in the individual publication describes the degree and nature of compliance required.

Directory Information Tree (DIT)—A directory information base organizational model that uses a hierarchical tree structure.

Directory—(1) In programming, a record containing details of the location of a file held in backing storage that is accessed by the operating system. (2) In databases, a file that stores relationships between records in other files. (3) In data communications, a table containing routine information.

Discretionary Access Control (DAC)—Means of restricting access to objects based on the identity and need- to-know of users and/or groups to which the object belongs. Controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (directly or indirectly) to any other subject.

Discretionary Protection—Access control features that identify individual users and their need-to-know and limits them to certain, specified information. See Discretionary Access Control.

Discretionary Security Protection—Trusted computing base that provides elementary discretionary access control protection (Class C1) features that separate users from data. It incorporates some form of credible controls capable of enforcing access limitations on an individual basis (i.e., suitable for allowing users to be able to protect private data and to keep other users from accidentally reading or destroying that data).

Discriminator—That part (stage) of a frequency modulation (FM) radio receiver that extracts the desired intelligence signal from an incoming FM carrier wave by changing frequency variations of the signal into amplitude variations (baseband or audio signals). Opposite of a modulator in a FM radio transmitter.

Disk Cache—In computers, a section of main memory or memory on the disk controller board. It bridges the disk and central processing unit (CPU), allowing faster disk access.

Disk Operating System (DOS)—(1) An operating system for computers with disk drives in which relevant routines are loaded from disk as required. (2) A program that controls the way programs are loaded into memory, how information is stored on the disk, and how the computer communicates with peripheral devices.

Diskless Workstation—A workstation that does not have a fixed (hard) or removable (floppy) disk drive. It is essentially a smart terminal that handles only presentation management. All processing and storage of interim data reside on the server. Diskless workstations can provide a better measure of cost efficiency and security than other end-user processing platforms.

Display Equipment—Any device that displays miniaturized information or documents, such as cathode ray tube displays or microform viewers.

Disposition Instructions—Precise instructions, specifying the date or event for cutoff, transfer, retirement, or destruction of records.

Disposition—(1) A comprehensive term that includes destruction, salvage, or donation; transfer to a staging area or records center; transfer from one organization to another. (2) Actions taken with inactive records. These actions may include erasure of data, transfer to a records center, or transfer to the National Archives.

Distributed Database—(1) A database that is not stored in a central location but is dispersed over a network of interconnected computers. (2) A database under the overall control of a central database management system but whose storage devices are not all attached to the same processor. (3) A database that is physically located in two or more distinct locations.

Diversity Reception—That method of radio frequency (RF) reception where, in order to minimize the effects of fading, a resultant signal is obtained by combination or selection, or both, of two or more independent RF signals that carry the same modulation or intelligence. Used primarily in microwave radio systems. Examples of diversity are frequency, space, and polarization diversity.

Document—Recorded information on paper or other medium.

Document Conversion—The act of converting paper records to another media. (Paper is still the official record media; conversion to another media for storage may require National Archive approval).

Document Reader—A device capable of reading documents into a computer.

Documentation—(1) The act or process of substantiating by recording actions and/or decisions. (2) Records required to plan, develop, operate, maintain, and use electronic records and software. Included are systems specifications, file specifications, codebooks, record layouts, user guides, and output specifications.

DoD Trusted Computer System Evaluation Criteria (TCSEC)—Document containing basic requirements and evaluation classes for assessing degrees of effectiveness of hardware and software security controls built into an Information System. This document, DoD 5200.28 STD, is commonly referred to as the Orange Book.

Domain—(1) The independent variable used to express a function. Examples of domain are time, frequency, and space. (2) In distributed networks, all the hardware and software under the control of a specific set of one or more host processors.

Domain Name—The unique name that identifies an Internet site. Domain names always have two or more parts, separated by dots. A given machine may have more than one domain name, but a given domain name points only to one machine.

Domain Name System (DNS)—A stable and widely deployed component of the Internet. It is a static, hierarchical database used with Transfer Control Protocol/Internet Protocol hosts, and is housed on a number of servers on the Internet; it allows users to specify remote computers by host names rather than numerical Internet Protocol addresses.

Dominate—Term used to compare communications and information system security levels. Security level S1 is said to dominate security level S2 if the hierarchical classification of S1 is greater than, or

equal to, that of S2 and the non-hierarchical categories of S1 include all those of S2 as a subset.

Dot Matrix—(1) In computer graphics, a two-dimensional pattern of dots used for constructing a display image. This type of matrix is used to represent characters by dots. (2) In printing, a pattern of dots used as the basis for character formation in a matrix printer.

Dot Pitch—In peripherals, the distance between two corresponding dots in two adjacent triads.

Double Density—In memory systems, a technique to increase the storage capacity of a floppy disk. The packing density is increased by modified frequency modulation recording techniques.

Double Sideband—In radio communications, the frequency bands occupied by a modulated carrier wave, above and below the carrier frequency.

Double Sided—In memory systems, pertaining to a technique to increase the total storage capacity of a floppy disk by recording data on both sides of the disk.

Down-Converter—In radio communications, a device, generally in the receiving equipment, which translates or converts the input signal frequencies in such a manner that the output frequencies are lower in the spectrum than the input frequencies. The frequency translation process does not alter the intelligence contained in the input signal.

Downlink—In satellite communications, that portion of a satellite link involving transmission of a signal from the satellite to the earth terminal. It is the opposite of uplink.

Drivability—In data communications, refers to the ease with which users may transfer from one application to another with minimal interference, errors, confusion, relearning, or retraining. Drivability relates only to those aspects for which consistency is necessary to promote easy transfer among conforming environments.

Drop Accountability—Procedure under which a communications security (COMSEC) account custodian initially receipts for COMSEC material, and then provides no further accounting for it to its central office of record. Local accountability of the COMSEC material may continue to be required.

Dual Diversity—The simultaneous combining of (or selection from) two independently fading signals, so that the resultant signal can be detected through the use of space, frequency, angle, time, or polarization characteristics.

Dumb Terminal—In peripherals, a terminal (or computer using dumb terminal software) that allows communications with other computers, but does not enhance the data exchanged or provide additional features.

Duplex Cable—A fiber optic cable composed of two fibers.

Duplex Circuit—In telecommunications, a circuit that permits transmission in both directions, but not simultaneously. For simultaneous two-way transmission, see Full-Duplex Circuit.

Duplexer—In radio communications, a three-port frequency dependent device used to separate or combine radio frequency signals. It allows simultaneous transmission and reception of two signals of different frequencies using a single antenna system with isolation between the two signals.

Durability—The probability that an item of equipment or system will perform its intended function for a specified interval under stated conditions without major failures.

Dynamic Random Access Memory (DRAM)—In a computer, a random access data storage method in

which the memory cells require periodic electrical refreshing to avoid loss of data held. DRAM is erasable and reprogrammable. DRAM will lose its contents when the power is removed (volatile memory).

E & M Signalling—In telephony, a signaling arrangement characterized by the use of separate paths for the signaling and the voice signals. The M lead (derived from "Mouth") transmits ground or battery from the distant end of the circuit, while incoming signals are received as either a grounded or open condition on the E (derived from "Ear") lead.

Earth Coverage—In satellite communications, the coverage that occurs when a radio beam from the satellite is sufficiently wide to cover the surface of the earth exposed to the satellite.

Earth Segment—The earth segment includes all equipment not in space orbit and capable of communicating with a satellite. Such equipment may be airborne, shipborne, or land-based and includes equipment used for operational communications and for satellite control.

Earth Station—A station located either on the earth's surface or within the major portion of the earth's atmosphere and intended for communication with one or more space stations, or with one or more stations of the same kind by using one or more reflecting satellites or other objects in space.

Economic Assessment—Comparison of the benefits of proposed security measures versus their cost. An economic assessment aids in planning and selecting security measures.

Edit—To change, add, delete, or move individual blocks of data in a database.

Effective Radiated Power (ERP)—In a radio transmission system, the signal power supplied to the antenna multiplied by the power gain of the antenna in a given direction.

Electrically Alterable Read-Only Memory (EAROM)—A read-only memory that can be modified electrically while connected in-circuit. Synonymous with **Electrically Erasable Read-Only Memory**.

Electrically Erasable Programmable Read-Only Memory (EEPROM)—A special kind of ROM that can be electrically erased and reprogrammed.

Electroabsorbtion Modulator (EAM)—In long-haul optical fiber communications, a semiconductor device that improves optical signal detection.

Electromagnetic Axis—An imaginary line emanating from an antenna that is coincident with the maximum field intensity of the antenna pattern in free space (i.e., without the influences of the earth's atmosphere and effects of objects.

Electromagnetic Compatibility (EMC)—(1) The ability of systems, equipment, and devices that use the electromagnetic spectrum to operate in their intended operational environments without suffering unacceptable degradation or causing unintentional degradation because of electromagnetic radiation response. It involves the application of sound electromagnetic spectrum management and system/ equipment/device design configuration to ensure interference-free operation. (2) The condition that prevails when telecommunications equipment is performing its individually designed function in a common electromagnetic environment without causing or sufferng unacceptable degredation due to intentional electromagnetic interference to or from other equipment in the same environment.

Electromagnetic Deception—The deliberate radiation, re-radiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an enemy or to enemy electromagnetic-dependent weapons, thereby degrading or

neutralizing the enemy's combat capability.

Electromagnetic Environmental Effects (E3)—E3 is the impact of the electromagnetic environment upon the operational capability of military forces, equipment, systems, and platforms. It encompasses all electromagnetic disciplines, including electromagnetic compatibility and electromagnetic interference; electromagnetic vulnerability, electromagnetic pulse protection; hazards of radiation to personnel, ordnance, and volatile materials; and natural phenomena effects of lightning and static discharges.

Electromagnetic Expendables—Nonrecoverable electronic warfare devices, such as chaff, flares, unmanned vehicles, decoys, and unattended jammers.

Electromagnetic Interference (EMI)—Any electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance or electronic/electrical equipment. It can be induced intentionally, as in some forms of electronic warfare, or unintentionally, as a result of spurious emissions and responses, intermodulation products, and the like.

Electromagnetic Intrusion—The intentional insertion of electromagnetic energy into transmission paths in any manner, with the objective of deceiving operators or of causing confusion.

Electromagnetic Jamming—The deliberate radiation, re-radiation, or reflection of electromagnetic energy to prevent or reduce the enemy's effective use of the electromagnetic spectrum, and with the intent of degrading or neutralizing the enemy's combat capability.

Electromagnetic Radiation (EMR) Hazards—Hazards caused by a transmitter/antenna installation that generates electromagnetic radiation in the vicinity of ordnance, personnel, or fueling operations in excess of established safe levels or increases the existing levels to a hazardous level; or a personnel, fueling, or ordnance installation located in an area that is illuminated by electromagnetic radiation at a level that is hazardous to the planned operations or occupancy.

Electromagnetic Spectrum—The total range of frequencies, from zero to infinity, over which any form of electromagnetic radiation occurs. The lowest frequencies are radio waves; increases in frequency produce infrared, visible light, ultraviolet, x-rays, gamma radiation, and cosmic rays. The electromagnetic spectrum was, by custom and practice, formerly divided into 26 alphabetically designated bands. This usage still prevails to some degree; however, the International Telecommunications Union formally recognizes 12 bands from 30 hertz to 3000 gigahertz. New bands from 3 THz to 3000 EHz are under consideration.

Electromagnetic Wave—An energy wave produced by the simultaneous periodic variation of electric and magnetic fields. Electromagnetic waves include radio waves, infrared, visible light, ultraviolet, X-rays and gamma rays.

Electronic Attack—Electronic warfare activities designed to prevent or reduce an adversary's effective use of the electromagnetic spectrum. Formerly called Electronic Countermeasures.

Electronic Bulletin Board (EBB)—(1) A system that connects users and a common computer host. Used to exchange software programs, technical information, and other information and data. (2) A computer with software that permits individuals to dial up via modem and exchange electronic mail messages with other users of the system. Bulletin boards are frequently composed of news groups that share information on a wide range of topics.

Electronic Business/Electronic Commerce (EB/EC)—(1) The interchange and processing of information via electronic techniques for accomplishing transactions based upon the applications of

commercial standards and practices. (2) The conducting of business communications and transactions over networks and through computers. As most restrictively defined, EB/EC is the buying and selling of goods and services, and the transfer of funds, through digital communications. EB/EC also includes all intercompany and intracompany functions (such as marketing, finance, manufacturing, selling, and negotiation) that enable commerce and use electronic mail, electronic data interchange, file transfer, facsimile, video conferencing, workflow, or interaction with a remote computer (including use of the World Wide Web).

Electronic Data Interchange (EDI)—The computer-to-computer exchange of business documents in a standard format by a computer-based communications system. This business procedure replaces paper versions of a variety of business documents such as purchase orders, shipping notices, invoices, receipts, inventories, payments, etc.

Electronic Data Interchange for Administration, Commerce, and Transport (EDIFACT)—A United Nations-sponsored global set of EDI standards. EDIFACT is derived from the X.12 standards but incorporates additional and different segments and uses a more flexible and generic approach to defining data elements using qualifier code.

Electronic Data Processing—Data processing performed largely by electronic equipment.

Electronic Imaging—The collection, processing, storage, retrieval, and exploitation of images through electronic means. The term includes digital photography, computer generated graphics and video images.

Electronic Interoperability—A special form of interoperability where two or more electronic equipment, especially communications equipment, can be linked together, usually through common interface characteristics and so operate the one to the other. See also: Interoperability.

Electronic Key Management System (EKMS)—Interoperable collection of systems being developed services and agencies of the U.S. Government to automate the planning, ordering, generating, distributing, storing, filling, using, and destroying of electronic key and management of other types of communications security material.

Electronic Mail (E-mail)—(1) The information exchanged between individuals or organizations by means of application of computer-to-computer data transfer technology, normally as textual messages. (2) Communication processed through a network, from one workstation to another.

Electronic Messaging Services—Services providing interpersonal messaging capability; meeting specific functional, management, and technical requirements; and yield a business-quality electronic mail service suitable for the conduct of official government business.

Electronic Printing—Electronic composition, reproduction, and finishing of information for general distribution produced through high-speed imaging without a plate, using nonimpact methods on paper, film, magnetic, or optical media.

Electronic Protection—That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability.

Electronic Private Branch Exchange (EPBX)—In telecommunications, electronic processors controlled with either space-division or time-division switching. Provides the same services as a private branch exchange but with manual operations accomplished by cordless consoles instead of cord-type switchboards.

Electronic Publishing—An electronic means for providing all aspects of the document publishing process, including creation, text and graphics design and capture, editing, storage, transfer, printing, and distribution.

Electronic Record—Any combination of text, graphics, data, audio, pictorial, or other information represented in digital form, that is created, modified, maintained, archived, retrieved, or distributed by a computer.

Electronic Security—Protection resulting from measures designed to deny unauthorized persons information derived from the interception and analysis of noncommunications electromagnetic radiations.

Electronic Security Assessment—One of three levels of capability to improve communications-computer systems security posture by accurately measuring the posture and recommending countermeasures where deficiencies exist.

Electronic Signature—A computer compilation of any symbols or series of symbols executed, adopted, or authorized by an individual to indicate the person's identity. Electronic signatures include digitized images of paper-based signatures, typed notations, the address information in an e-mail header, and digital signatures. Electronic signatures may or may not be linked to a form or document.

Electronic Transaction System—A web-based system used to access all Air Force and subordinate electronic publications and forms and to place orders for physical products.

Electronic Warfare (EW)—Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within EW are: electronic attack, electronic protection, and electronic warfare support.

Electronic Warfare Support—That division of electronic warfare involving actions taken by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition.

Electronically Generated Key—Key generated in a communications security device by introducing (either mechanically or electronically) a seed key into the device and then using the seed, together with a software algorithm stored in the device, to produce the desired key.

Element—Removable item of communications security equipment, assembly, or subassembly that normally consists of a single piece or group of replaceable parts.

Emanation—Unintended signals or noise radiated by and appearing external to electronic equipment.

Embedded Computer System—A computer system that is integral to a larger system whose primary purpose is not computational. An embedded computer would require major modifications in order to be used for general-purpose computing and is managed as a component of the system in which it is embedded.

Embedded Cryptographic System—Cryptosystem performing or controlling a function as an integral element of a larger system or subsystem.

Embedded Cryptography—Cryptography engineered into an equipment or system whose basic function is not cryptographic.

Emission Control—The selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: (a) detection by

enemy sensors; (b) minimize mutual interference among friendly systems; and/or (c) execute a military deception plan.

Emission Security (EMSEC) Assessment—An evaluation of a facility to determine the need for emission security.

Emission Security—Protection resulting from measures taken to deny unauthorized persons information derived from intercept and analysis of compromising emanations from cryptoequipment or an information system.

Emulator—In computing, special-purpose hardware or software that enables one system to act as if it were another. It is used, for example, to minimize reprogramming efforts when a new computer replaces an existing one.

Encapsulating Security Protocol (ESP)—A security protocol which provides data privacy services, optional data authentication, and anti-replay services. ESP encapsulates the data to be protected.

Encipher—Convert plain text to cipher text by means of a cryptographic system.

Encode—Convert plain text to cipher text by means of a code.

Encrypt—(1) To convert plain text into unintelligible form by means of a cryptosystem. (2) Generic term encompassing encipher and encode.

Encryption Algorithm—Set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key.

End-Fire Array—Antenna An antenna consisting of a linear array of radiators in which the maximum radiation is along the axis of the array; the antenna may be uni- or bi-directional.

End Instrument—In telecommunications, a device connected to the terminal of a circuit and used to convert usable intelligence into electrical signals or vice-versa.

End Item—A final combination of end products, component parts, or materials that is ready for its intended use. In the C4 world, a complete communications system (as well as a subsystem or main component such as a radio transmitter, receiver, antenna system, etc.) can be designated as an end item.

End-Item Accounting—In information assurance, the accounting for all the accountable components of communications security equipment configuration by a single short title.

End Office (EO)—An integral part of the Defense Switched Network (DSN). An EO provides switched call connections and all DSN service features, including multi-level precedence and preemption. The EO provides long distance service by interconnection with multifunction switches. The EO does not serve as a tandem in the DSN, but may connect to other EOs where direct traffic volume requires using a community of interest trunk. As part of the DSN, EOs will be interconnected to and supervised by the DSN system control subsystem.

Endorsed Data Encryption Standard (DES) Equipment—Unclassified equipment that embodies unclassified data encryption standard cryptographic logic and has been endorsed by the National Security Agency for the protection of national security information.

Endorsed for Unclassified Cryptographic Item—Unclassified cryptographic equipment that embodies a U.S. Government classified cryptographic logic and is endorsed by the National Security Agency for the protection of national security information.

Endorsement—National Security Agency approval of a commercially-developed product for safeguarding national security information.

End-To-End Encryption—Encryption of information at its origin and decryption at its intended destination without intermediate decryption.

End-To-End Security—Safeguarding information in an information system from point of origin to point of destination.

End-User Devices—Information system terminal components (for example, workstations, telephones, sensors, displays, and radios) which are used to enter date, extract information, or control processing and transfer; functional end-user organizations generally control these resources.

Engineering Data—Data required to define and document an engineering design or product configuration sufficiently to allow duplication of the item.

Enhanced Telephony—Enhanced telephony environments provide improved means of using the telephone system for interactive audio exchanges between users. Features include: call forwarding, call waiting, programmed directories, teleconferencing capability, automatic call distribution, and call detail recording.

Enterprise—Relative to DoD Chief Information Officer (CIO) guidance and policy, an enterprise is any of the following: The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities.

Entrapment—Deliberate planting of apparent flaws in an communications and information system for the purpose of detecting attempted penetrations.

Envelope Delay—In telecommunications, envelope delay refers to the characteristics of a circuit that cause certain frequencies to be delayed more than others resulting in distortion of the overall frequency envelope at the receiving end.

Envelope—In a message handling system, the part of a message that contains information necessary to deliver the message to the recipient. In addition, the envelope may contain information that identifies the message originator and potential recipients, records details of the routing by the message transfer system, and characterizes the message content.

Ephemeris—A table or listing of the predicted positions of celestial bodies, such as of the planets in our solar system, to include artificial satellites orbiting the earth.

Equalization—The process of reducing frequency distortion and, or phase distortion of a circuit by the introduction of networks to compensate for the difference in attenuation and, or time delay at the various frequencies in the transmission band.

Equalizer Delay—In telecommunications, a corrective network used in a circuit for the purpose of compensating for the phase delay and envelope delay characteristics of the circuit and making these delays substantially constant over the desired frequency range thereby minimizing distortion of the signals.

Equatorial Orbit—For a satellite orbiting the earth, an orbit in the equatorial plane.

Equipment Item—In logistics, end items that do not become components of higher-level assemblies.

Equipment Radiation Tempest Zone (ERTZ)—A zone established as a result of determined or known

equipment radiation TEMPEST characteristics. The zone includes all space within which a successful hostile intercept of compromising emanations is considered possible.

Equipment Reliability—The percent of time a specific equipment component was operational during a specified period of time.

Erasable Programmable Read-Only Memory (EPROM)—ROM that is erasable and reprogrammable. This type of ROM is usually erased off-circuit, usually by exposure to an ultraviolet light source.

Erase—To replace all the binary digits in a storage device by binary zeros.

Erasure—Process intended to render magnetically stored information irretrievable by normal means.

Erlang—A unit of telecommunications traffic intensity determined by the product of the number of calls carried by the circuit and the average duration of the call in hours.

Error Correcting Code (ECC)—A code designed to detect an error in a word or character, identify the incorrect bits, and replace them with the correct ones.

Error Rate—The ratio of the number of bits, elements, characters, or blocks incorrectly received to the total number of bits, elements, characters, or blocks transmitted in a specified time interval.

Ethernet—A baseband local area network specification developed jointly by Digital Equipment Corporation, Xerox, and Intel to interconnect computer equipment using coaxial cable and transceiver

European Telephone System (ETS)—The military telephone system in Europe that uses digital telephone switches. ETS is part of the Defense Switched Network.

Evaluated Products List (EPL)—Equipment, hardware, software, and/or firmware evaluated by the NCSC in accordance with DoD TCSEC and found to be technically compliant at a particular level of trust. The EPL is the National Security Agency Information Systems Security Products and Services Catalogue.

Evaluation—The review and analysis of qualitative or quantitative data obtained from design review, hardware inspection, testing, or operational use of equipment.

Exa(E)—A prefix used to denote 10^{18}.

Exahertz (EHz)—A unit denoting 10^{18} Hz.

Exercise Key—Key used exclusively to safeguard communications transmitted over-the-air during military or organized civil training exercises.

Exhaustive attack—An attempt to break a code or to find a key or password by using methods that are primarily random (trial-and-error) in nature, as opposed to analytical methods.

Expanded Binary Coded Decimal Interchange Code (EBCDIC)—(1) An 8-bit code used to represent 256 unique letters, numbers, and special characters. (2) The standard representation of numbers and letters by IBM computers.

Exploitable Channel—Channel that allows the violation of the security policy governing an communications and information system and is usable or detectable by subjects external to the trusted computing base. See Covert Channel.

Extended Industry Standard Architecture (EISA)—In computers, a standard bus (interconnection) architecture that extends the ISA standard to a 32-bit interface.

Extensible Markup Language (XML)—A recognized International Organization of Standardization (ISO) standard to structure information in electronic documents according to content and structure rather than format. It is a subset, or abbreviated version, of the Standard Generalized Markup Language (SGML) tailored for use on the world wide web. XML omits the more complex and lesser used parts of SGML.

Extensible Name Service (XNS)—An open protocol and open-source platform for universal addressing, automated data exchange, and privacy control. XNS is based on two key technologies: Extensible Markup Language (XML), the global standard for platform-independent information exchange, and web agents, a patented technology that automates the exchange, linking, and synchronization of information between publishers and subscribers over digital networks. XNS provides web agents with a common XML vocabulary to "speak," as well as a global naming and addressing service for finding each other on the Internet. XNS combines XML and web agents to create a complete, integrated infrastructure for automated information exchange between consumers and business anywhere on the wired or wireless Internet.

Exterior Gateway Protocol (EGP)—The service by which gateways exchange information about what systems they can reach.

External Environment Interface (EEI)—The interface between the application platform and the external environment across which information is exchanged. The EEI is defined primarily in support of system and application interoperability.

Extraction Resistance—Capability of crypto equipment or secure telecommunications equipment to resist efforts to extract key.

Extraterrestrial Noise—Random noise originating in outer space and detected on the earth.

Extremely High Frequencies (EHF)—Frequencies of electromagnetic waves ranging from 30-300 GHz.

Extremely Low Frequencies (ELF)—Frequencies of electromagnetic waves below 300 hertz.

F—A term used in used in publication footnotes and product announcements meaning Functional Distribution.

Facsimile (fax)—A system of telecommunications for transmitting fixed images (e.g., pictures, drawings, text, etc.) with a view to their reception in a permanent form.

Fading—In radio communications, fluctuations in the strength of received radio signals because of variations in the transmission medium. These variations are generally due to atmospheric, electromagnetic, and/or gravitational influences that cause the radio signals to be deflected or diverted away from the receiving antenna.

Fail Safe—Automatic protection of programs and/or processing systems when hardware or software failure is detected.

Fail Soft—Selective termination of affected nonessential processing when hardware or software failure is determined to be imminent.

Failure Access—Unauthorized access to data resulting from hardware or software failure.

Failure Control—Methodology used to detect imminent hardware or software failure and provide fail safe or fail soft recovery.

Family-of-Systems (FoS)—A set or arrangement of independent systems that can be arranged or

interconnected in various ways to provide different capabilities. The mix of systems can be tailored to provide desired capabilities on the situation.

Federal Information Processing (FIP) Resources—Any automated data processing equipment (ADPE).

Federal Information Processing Standards (FIPS)—Issued by the National Bureau of Standards, they announce the adoption and implementation of specific information systems standards and guidelines within the Federal Government.

Federal Telecommunications System (FTS)—A general-purpose, nationwide, nonsecure voice communications network managed and operated by the Government Services Administration. It supports the essential needs of Federal Government departments and agencies. The FTS provides local, long-line (intercity), and commercial interface service to its subscribers.

Feedback—In electronics, the return of a portion of the output signal to a previous or input stage of a circuit or device, typically an amplifier. By controlling its magnitude and phase, the feedback signal is used to influence the operating parameters of the circuit or device, such as gain, stability, distortion, and linearity.

Femto (f)—A prefix used to denote one quadrillionth (10^{-15}).

Fiber Crosstalk—In opto-electronics, the exchange of light wave energy between the core and the cladding of a fiber optic cable, the cladding and the ambient surrounding, or between different indexed layers. The crosstalk is deliberately reduced by making the cladding loose.

Fiber Distributed Data Interface (FDDI)—A standard of transmitting data on optical fiber cables at a rate of around 100 Megabits-per-second.

Fiber Optics—The technology of using thin glass or plastic filaments to transmit signals as pulses of light at frequencies of about 10^{14} hertz. The filament acts as a wave guide for the light, reflecting it back and forth from the inside walls, allowing it to be transmitted around bends and over long distances with minimal loss.

Field Programmable Gate Array (FPGA)—FPGAs are basically blank silicon computer chips made up of millions of transistors and gates that can be reprogrammed an infinite number of times, even while the device is running. FPGAs are used in the new generation of hypercomputers instead of microprocessors for its computing power.

Field—The term for an item on a form, such as a name or address. Fields form records in a file or database.

Figure—An illustration such as a map, drawing, photograph, graph, or flow chart, or other pictorial device inserted into a publication. Additionally, a figure can also be an illustration that is set in type such as a sample format or memorandum.

File Allocation Table (FAT)—In computing, a table used by the operating system to allocate space on a magnetic disk for a file. The sectors allocated may be randomly scattered over the disk and the table locates and chains together the sectors for each file.

File Format—In computing, the structure or arrangement of data stored in a file. Applications always store data files in a particular format. A format readable by one application may not be readable by another.

File Protection—Aggregate of processes and procedures designed to inhibit unauthorized access, contamination, elimination, modification, or destruction of a file or any of its contents.

File Security—Means by which access to computer files is limited to authorized users only.

File Server—(1) A computer with connectivity to more than one user, used as a centralized information storage device. This system allows users to exchange data, applications software, and files. The file server may have software packages for electronic mail, calendars, system administration, and so forth. (2) The file server provides transparent access to files from workstations and other clients. Unlike a data server, the file server provides access and linkage to the file directories and is not aware of the contents of the file. Processing of the contents of the file needs to be performed by the client. The file server does no client visible manipulation of the data within a file. Essentially, the file server provides the client with the use of a virtual disk drive and little else. In a workstation environment, the workstation would perform all the processing on the file.

File Transfer Protocol (FTP)—A Transmission Control Protocol/Internet Protocol (TCP/IP) application program used to transfer files from one computer to another. It is commonly used on the Internet.

File—(1) In data structures, a collection of records that are logically related to each other and handled as a unit (for example, by giving them a single name). (2) A grouping of data in a named entity, under a file name, organized into special, ordinary, or directory files. (3) In electronic recordkeeping, an organized collection of related data, usually arranged into logical records that are stored together and treated as a unit.

Fill Device—Communications security item used to transfer or store key in electronic form or to insert key into a crypto equipment.

Filter—An electrical or electronic device or network that passes desired frequencies, but blocks or greatly attenuates others. There are two basic types, active and passive filters. Active filters require the application of electrical power for the utilization of their filtering properties, passive filters do not.

Finger—An internet software tool for locating people on other Internet sites. Finger is also sometimes used to give access to non-personal information, but the most common use is to see if a person has an account at a particular Internet site. Not all sites allow incoming finger requests.

Firefly—Key management protocol based on public key cryptography.

Firewall—In computer networking, (1) A special kind of router that filters network traffic, in addition to connecting two networks together. (2) A combination of hardware and software that separates a Local Area Network (LAN) into two or more parts for security purposes.

Firmware—(1) Software that is permanently stored in a hardware device that allows reading but not writing or modifying the software. The most common device used for firmware is read-only memory. (2) The combination of a hardware device and computer instructions or data that reside as read-only software on the hardware device. The software cannot readily be modified under program control.

Firmware—Program recorded in permanent or semi-permanent computer memory.

First Generation Language—In programming, a machine code or assembly language.

First In-First Out (FIFO)—An algorithm used in determining the order of handling or consideration. At any one time, the next item to be dealt with is that item among a group of items that has been waiting the longest. It is the inherent structure of a queue.

Five-Year Interoperability Assurance Plan (FYIAP)—A Joint Chiefs of Staff (JCS) program managed by Joint Interoperability Test Center (JITC) that documents requirements for C4 interoperability certification, recertification, requalification, and revalidation testing. The FYIAP, published annually in January, establishes the C4 interoperability testing and certification program.

Fixed communications security (COMSEC) Facility—COMSEC facility located in an immobile structure or aboard a ship.

Flash—A specific family of EEPROM devices that hold their content without power. It can be erased in fixed blocks rather than single bytes. Block sizes range from 512 bytes up to 256 kbps.

Flaw Hypothesis Methodology—System analysis and penetration technique in which the specification and documentation for an communications and information system are analyzed to produce a list of hypothetical flaws. This list is prioritized on the basis of the estimated probability that a flaw exists on the ease of exploiting it, and on the extent of control or compromise it would provide. The prioritized list is used to perform penetration testing of a system.

Flaw—Error of commission, omission, or oversight in an communications and information system that may allow protection mechanisms to be by-passed.

Flexible, Modular C4 Packages—Flexible, modular C4 packages consist of compatible and interoperable hardware, software, and database modules and appliqués. Examples include rugged, lightweight, small hardware for mobile and transportable use; easily configured shelters and equipment for start-up, operation, and removal.

Font—A family, set, or particular assortment of consistent size, shape, or style of print characters.

Footprint—In satellite communications, that portion of the earth's surface illuminated by a narrow radio frequency signal beam from a satellite; it is less than earth coverage.

Formal Access Approval—Documented approval by a data owner to allow access to a particular category of information.

Formal Cryptographic Access (FCA)—Formal approval permitting access to COMSEC keying material and prior consent to a non-lifestyle, counterintelligence-scope polygraph examination.

Formal Development Methodology—Software development strategy that proves security design specifications.

Formal Proof—Complete and convincing mathematical argument presenting the full logical justification for each proof step and for the truth of a theorem or set of theorems. These formal proofs provide A1 and beyond A1 assurance under the DoD Trusted Computer System Evaluation Criteria (Orange Book).

Formal Security Policy Model—Mathematically precise statement of a security policy. Such a model must define a secure state, an initial state, and how the model represents changes in state. The model must be shown to be secure by proving that the initial state is secure and that all possible subsequent states remain secure.

Formal Top-Level Specification—Top-level specification written in a formal mathematical language to allow theorems, showing the correspondence of the system specification to its formal requirements, to be hypothesized and formally proven.

Formal Verification—Process of using formal proofs to demonstrate the consistency between formal specification of a system and formal security policy model (design verification) or between formal

specification and its high-level program implementation (implementation verification).

Format—(1) Arrangement of bits or characters within a group, such as a word, message, or language. (2) Shape, size, and general make-up of a document. (3) A guide, table, sample, or exhibit that illustrates a predetermined arrangement or layout for presenting data. A format may or may not be a form.

Forms—A form is a predetermined arrangement of captioned spaces, developed for collecting, recording, and extracting information in a standardized order. The form may exist on paper or film negative, be programmed in computer language, or displayed on a video terminal. Number forms for easy reference and effective management; and prescribe them in publications, to ensure maximum efficiency and effectiveness.

Formula Translator (FORTRAN)—A high-level programming language initially designed for scientific applications, but now used for many commercial and industrial applications.

FORTEZZA—The name given to the Personal Computer Memory Card International Association (PCMCIA) card used in the encryption and authentication of defense message system messages.

Fortuitous Conductor—Any conductor that may provide an unintended path for electrical signals (for example, water pipes, metallic structural members, etc.).

Forward Error Correction—The use of an error-correcting code to automatically correct some or all of the signals detected as being in error before they arrive at the data sink.

Forward Scatter—Radio wave propagation in which the direction of the incident wave and the scattered wave lie in or near a great circle plane containing the transmit and receive antennas. The term scatter can be applied to reflection or refraction by relatively uniform media, but is usually taken to mean propagation in which the wavefront and direction are modified in a relatively disorderly fashion.

Fourth-Generation Language—A computer programming language (of an order higher than high-order programming languages) designed for easy use by personnel with minimal data processing experience or training to retrieve information from an existing computer application system or quickly develop application software systems or portions of software systems.

Four-Wire Circuit—In telecommunications, a two-way transmission circuit using four connections (wires); one pair to transmit and one pair to receive.

Frame—1. A single display image or screen on a monitor. 2. In a time division multiplexing system, a frame is a repetitious group of signals resulting from a single sampling of all channels, and including any additional signals for synchronization and other required system information.

Frame Frequency—The number of times per second a frame of information is transmitted or received.

Frame Relay—A packet mode service, a network access protocol for bursty data applications. It is a standard interface specification optimized for transport protocol-oriented traffic. Frame relay can improve on other protocols, such as X.25, local area network bridges, and routers, and help further optimize network resources.

Framing Bit—A bit at a specific recurring interval in a bit stream used to denote the beginning or end of a frame (a predetermined group of bits). A bit used for frame synchronization. In a bit stream, framing bits are noninformation bits.

Free Space—Empty space with no free electrons or ions present. The term also implies remoteness from material objects that could cause reflection of radio waves.

Frequency Allocation—The designation of frequency bands for use in performing specific functions or services.

Frequency Assignment—The process of designating a specific frequency for use at a particular station for specified operating conditions.

Frequency Coordination—In frequency spectrum management, the process of obtaining approval to use the radio frequency spectrum via arrangements and technical liaison for the purpose of minimizing harmful interference through cooperative use of the radio frequency spectrum.

Frequency Deconfliction—A systematic management procedure to coordinate the use of the electromagnetic spectrum for operations, communications, and intelligence functions. Frequency deconfliction is one element of electromagnetic spectrum management.

Frequency Deviation—In a frequency modulated radio wave, the peak difference between the instantaneous frequency of the modulated wave and the carrier frequency.

Frequency Diversity—In telecommunications, a method to counteract the fading of a radio frequency (RF) signal over a radio link or path. The information signal is transmitted on (typically) two different carrier frequencies over the same link. Since fading is frequency selective, the two RF signals are less likely to fade at the same time; the stronger of the two signals is constantly selected thereby ensuring reception of the best possible signal.

Frequency Division Multiple Access (FDMA)—In satellite communications, the use of frequency division to provide multiple and simultaneous transmission to a single transponder.

Frequency Division Multiplexing (FDM)—In telecommunications, an analog modulation technique that allows the transmission of multiple signals simultaneously over a single transmission path, such as a cable or radio system. The multiple signals or channels are separated in frequency within the consolidated baseband.

Frequency Drift—A slow, undesired change in the frequency of an oscillator (in a transmitter or receiver).

Frequency Hopping—In radio communications, the periodic changing of the frequency or frequency set associated with a transmission. Successive frequency sets are determined by a pseudo noise code. A frequency hopping signal may be regarded as a sequence of modulated pulses with carrier frequencies that hop in a pseudo random pattern. The net effect is to spread the information over a wider bandwidth, thereby reducing the effects of jamming or interfering signals.

Frequency Modulation (FM)—In radio communications, a form of angle or phase modulation in which the instantaneous frequency of the sine wave carrier is caused to depart from its frequency by an amount proportional to the instantaneous value of the modulating signal, or simply, a low(er) frequency modulating a high(er) frequency. Compared to amplitude modulation (AM), an advantage of FM is its ability to suppress the effects of interfering signals resulting in improved signal-to-noise levels in the demodulated (typically audio/voice) signals. A disadvantage is FM requires much more bandwidth than AM and more complex transmitters and receivers.

Frequency Shift Keying (FSK)—A form of frequency modulation in which the modulating signal shifts the output frequency between predetermined values and in which the output signal has no phase discontinuity.

Frequency Tolerance—The maximum permissible departure by the center frequency of the frequency

band occupied by an emission from the assigned frequency, or by the characteristic frequency of an emission from the reference frequency expressed in Hz or parts per million (10^6).

Frequency Translation—The transfer en bloc of signals occupying a definite frequency band (such as a channel or group of channels) from one position in the frequency spectrum to another, in such a way that the arithmetic frequency difference of signals within the band is unaltered.

Frequency—The number of cycles per unit of time. In electrical/electronic applications, the measurement unit of a frequency is the hertz that is one cycle per second.

Front-End Processor—(1) A programmed-logic or stored program device that interfaces data communications equipment with an input/output bus or memory of a data processing computer. (2) In a computer network, a processor that relieves a host computer of processing tasks such as line control, message handling, code conversion, and error control.

Front-End Security Filter—Security filter logically separated from the remainder of an communications and information system to protect system integrity. Synonymous with **Firewall**.

Front-to-back Ratio—A ratio of parameters used in connection with antennas, rectifiers, or other devices in which signal strength, resistance or other parameters in one direction (of signal or current flow) is compared with that in the opposite direction. The resultant figure is an indicator of the electrical performance of the device.

Full Duplex (FDX) Circuit—In telecommunications, a circuit that permits transmissions in both directions simultaneously.

Full Operational Capability (FOC)—The full attainment of the capability to employ effectively a weapon, item of equipment, or system of approved specific characteristics, which is manned and operated by a trained, equipped, and supported military unit or force.

Functional Design Authority (FDA)—The final authority on a specific software and computer system assigned based on the designated requirement. The FDA is the advocate for all requirements for all users of the system. Only one FDA will be authorized for system approval and functional accountability in each of the 11 established functional domains (that is, organizations).

Functional Economic Analysis (FEA)—A structured proposal that serves as the principal part of a decision package for enterprise leadership. It includes an analysis of functional process needs or problems; proposed solutions, assumptions, and constraints; alternatives; life-cycle costs; benefits and, or cost analysis; and investment risk analysis.

Functional Model—A structured representation of the activities and functions performed by an organization and the information exchanged between them. This is a portion of architecture.

Functional Publication Library (FPL)—A unit or staff office library that contains only the publications needed for the mission in a specific functional area.

Fundamental Frequency—In electronics, the repetition frequency of one cycle of a complex, repetitive waveform.

Fusion—(1) The process of combining/aggregating data to derive a more complete assessment of a specific capability, action, or situation. (2) The process of receiving and integrating all-source, multimedia, and multiformat information to produce and make available to the user(s) an accurate, complete, and timely summary of essential information required for successful prosecution of operational

objectives. Fused information is more valuable than information received directly from separate, multiple sources to the degree that it provides a more complete whole of related information.

Fuzzy Logic—In mathematics, a form of logic in which the variables may assume a continuum of values between 1 and 0. All computers operate on a yes or no principle. Simply put, fuzzy logic is a software program that adds a "maybe" to the process that allows software to operate at a higher level of abstraction and handle conflicting commands.

G/T—In satellite communications, the ratio of antenna gain to noise temperature; it is an operating parameter used to characterize the performance of a ground station.

Gain—(1) In electronics, the ratio of output current, voltage, or power-to-input current, voltage, or power, respectively. Gain is usually expressed in decibels. (2) The degree to which the strength of a signal is increased when it passes through an amplifier, repeater, or antenna.

Galactic—In databases, pertains to data that is extensive and accessible from many places and by many applications.

Galactic Noise—Unidentifiable radio frequency (RF) signals originating in outer space which appear as background noise on a radio receiver.

Garbage In, Garbage Out (GIGO)—A phrase describing the observation that the output of a data system can be no more correct than data it receives as input.

Garble—An error in transmission, reception, encryption, or decryption that changes the text of a message or any portion thereof in such a manner that it is incorrect or undecryptable.

Gateway—(1) In satellite communications, (a) an earth terminal used for connectivity between a terrestrial station and a satellite communications system; (b) a ground station that acts as a relay between satellites. (2) In data communications, (a) equipment used to interface networks so that a terminal can communicate with a terminal or computer on another network; (b) A device for providing interconnection between networks with different communications protocols; a gateway converts one network's message protocol to the format used by another network's protocol. It can be implemented in hardware or software.

Generic Application Environment (GAE)—One of three information technology architecture building blocks. Describes types of information technology application and tools needed to support specific application systems. This is the primary building block in linking application systems back to the technology environment.

Generic Technology Platform (GTP)—A term used to describe the different types of delivery components that can be used to support information technology applications.

Geographical Information System (GIS)—A combination of digital mapping and database technology that allows the user to see data about items on a map. Commonly used to identify communications circuits or utilities of a given area (e.g., Air Force base). By clicking on a representation of a physical object, such as a building, the user can access progressively greater levels of detail about the facilities within the building, down to circuit or telephone numbers and their actual locations.

Geostationary Orbit—In satellite communications, a circular orbit of 42,242 kilometers' radius that lies in the plane of the equator. A satellite in its orbit appears to remain stationary to an observer on the ground.

Geosynchronous Orbit—In satellite communications, a circular orbit of 42,242 kilometers' radius that

does not lie in the equatorial plane. A satellite in this orbit will have the same period of rotation as the earth, but the inclination of the orbit, to the equatorial plane, means that to an observer on the earth's surface the position of the satellite changes with time.

Giga (G)—Prefix used to denote one billion (10^9).

Global Grid—An open systems architecture that provides global connectivity instantaneously on warrior demand. The global grid can support both vertical and horizontal information flow to joint and multinational forces.

Global Information Grid (GIG)—The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.

Global Information Grid (GIG) Systems—Integrated systems of doctrine, procedure, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control across the entire range of military operations.

Global Information Infrastructure (GII)—The worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. It encompasses a wide range of communications and information equipment, systems, and networks, to include the personnel who make decisions and handle the transmitted information.

Glomar Response—A reply made to a Freedom of Information Act request that neither confirms nor denies the existence or nonexistence of requested records.

Government Emergency Telecommunications Service (GETS)—A service offered by the Office of the Manager, National Communications System (OM-NCS), to meet national security and emergency preparedness (NS/EP) requirements for the use of public, defense, or federal telephone networks by federal, state, or local government and other authorized users. GETS provides emergency access and specialized processing in local and long-haul-distance telephone networks.

Government Furnished Materiel (GFM)—Government property which may be incorporated into or attached to an end item to be delivered under a contract or which may be consumed in the performance of a contract. It includes, but is not limited to, raw and processed material, parts, components, assemblies, and small tools and supplies.

Government Furnished Property (GFP)—Property in the possession of or acquired directly by the government, and subsequently delivered to or otherwise made available to the contractor.

Government Information Locator Service (GILS)—An automated on-line card catalog which identifies public information resources throughout the U.S. Federal Government, describes the information available in those resources, and provides assistance in obtaining the information.

Government Printing and Binding Regulations (GPBR)—GPBRs are issued by the Congressional Joint Committee on Printing.

Government Printing Office (GPO) Regional Printing Procurement Office (RPPO)—The GPO is the primary source of Federal printing and is managed by the Public Printer. The RPPOs are established by the Public Printer to buy Federal printing in their areas.

Government-Off-The-Shelf (GOTS)—(1) An item of hardware or software that has been produced by or for the government and is available for reuse. (2) Products for which the government owns the data rights, that are authorized to be transferred to other DoD or U.S. Government customers, and that require no unique modifications or maintenance over the life cycle of the product.

Graphical User Interface (GUI)—A system design that allows the user to affect commands, enter into transaction sequences, and receive displayed information through graphical representations of objects (for example, menus, screens, buttons, and so forth).

Graphics Adapter—An item of electronic hardware in a computer that controls the monitor.

Graphics Arts—The design, creation, and preparation of two- and three-dimensional visual aid products. Includes graphs, posters, and visual material for brochures, covers, television, motion pictures, printed publications, displays, presentations, and exhibits.

Ground—In communications-electronics, a conducting connection, whether intentional or accidental, by which an electric circuit or equipment is connected to the earth (ground) or to some relatively large conducting body that serves in place of the earth.

Ground Mobile Forces Satellite Communications (GMF SATCOM)—A multi-service program comprised of ground terminals that are characterized by ease of set-up for quick reaction, transportability, and flexibility of communications links. Provides critical multi-channel command and control transmission requirements between command echelons and the war-fighters.

Ground Potential—Having the same electrical potential as the earth, which is considered to be of a negative potential in accordance with electron flow theory.

Ground Return Circuit—A circuit in which the earth serves as one conductor of an electrical or electronic circuit.

Ground Wave—A radio wave that is propagated over the surface of the earth and ordinarily is affected by the presence of the ground (terrain) and, to a lesser extent, the lower atmosphere.

Groupware—Software and systems that help groups coordinate and communicate about work on which they are cooperating. Groupware may incorporate e-mail, shared databases, workflow software, conferencing software, and scheduling software.

Guard Band—In telecommunications, a narrow band of frequencies left vacant between allocated channels that is intended to minimize the possibility of mutual interference between adjacent channels.

Half Duplex Circuit—A circuit that affords communications in either direction, but only in one direction at a time.

Handshaking—Passing control characters between two devices to control the flow of information between the devices.

Hard Disk—A mass-storage magnetic medium that uses a rigid material disk for mass storage of data. Usually hard-disk systems are faster and can store many times more data than is possible on floppy disks

of the same physical size. Usually, the disk itself, along with the read/write head, is housed in a sealed enclosure to ensure against contamination. For some systems, hard disks are available as removable cartridges. Under appropriate conditions, the cartridge disks can be used for classified processing in a normal office environment.

Hardware—(1) The generic term dealing with physical items as distinguished from its capability or function such as equipment, tools, implements, instruments, devices, sets, fittings, trimmings, assemblies, subassemblies, components, and parts. The term is often used in regard to the stage of development, as in the passage of a device or component from the design stage into the hardware stage as the finished object. (2) In data automation, the physical equipment or devices forming a computer and peripheral components.

Hardware Architecture—Assemblage of a computer's internal components and its attached peripheral devices that determine its capability and its limitations.

Hardware Security—Equipment features or devices used in a computer system to preclude unauthorized data access or support a trusted computing base.

Hardwired Key—Permanently installed key.

Harmful Interference—Any emission, radiation, or induction that endangers the functioning of a radio navigation service or other safety services or that seriously degrades, obstructs, or repeatedly interrupts a radio communication service operating in accordance with the International Telecommunications Union Radio Regulations.

Hazard—In communications security, a measure of both the existence and the compromising nature of an emanation. A hazard exists only if compromising emanations are detectable beyond the inspectable space.

Hecto (h)—A prefix denoting one hundred (10^2).

Helios Noise—Interference to satellite communications caused by the sun when an orbiting satellite passes between the sun and a tracking ground station.

Hertz (Hz)—A unit of frequency equal to one cycle per second.

Heterochronous—A relationship between two signals such that corresponding significant instants do not necessarily occur at the same time. See also Mesochronous and Plesiochronous.

Heuristic—(1) Procedures that are designed to develop a plan or program that will obtain desired results or output as an improvement over current procedures. (2) A term applied to a problem solving technique in which experiences, guesses, and trial-and-error methods are used.

High Altitude Electromagnetic Pulse (HEMP)—The electromagnetic pulse produced when a nuclear detonation occurs essentially outside the earth's atmosphere at a height of greater than 30 km.

High Bit Rate Digital Subscriber Line (HDSL)—A new technology that extends the distance a T1 (1.544 Mbps) link can operate over copper wire before it requires a repeater to maintain signal integrity. This technology also boasts optical fiber quality bit error rates.

High Frequency (HF)—Frequencies of electromagnetic waves in the range of 3 MHz to 30 MHz. Also generally referred to as the short wave band.

High Level Data Link Control (HDLC)—A communications protocol defined for high-level, synchronous connections to X.25 packet networks. Similar in most respects to synchronous data link control. See also Synchronous.

High Level Language—Computer programming language that does not reflect the structure of any one computer or class of computers.

High Risk Environment—Specific location or geographic area where there are insufficient friendly security forces to ensure the safeguarding of communications and information system security equipment.

High Speed—A term applied to a data communications device or facility capable of handling more than 4,800 bits per second.

High Threat Environment—See High Risk Environment.

High-Order Programming Languages—Programming languages (of an order higher than assembly languages) designed for easy expression of a class of problems or procedures to achieve varying degrees of machine independence. These languages are designed for programming convenience rather than for easy generation of machine code instructions. The languages are intended to present procedures to an interpreter or compiler, which creates a machine language program or series of subroutines for a computer to execute.

Highway—In digital communications, (a) A major data transfer path within a computer or other functional unit. It typically consists of a number of wires or multi-conductor cable. Compare to trunk or bus. (b) A digital serial-coded bit stream with time slots allotted to each call on a sequential basis.

Historical (Transaction) File—1. A file containing relatively transient data, that, for a given application, is processed together with the appropriate master file. 2. A file of accumulated data from previous transactional updates the office of primary responsibility (OPR) keeps separately for historical purposes. A valid file of items the OPR uses with the master data input file to create a master data output file. A file identical in format and content to a master file, that the OPR keeps separately for security backup, historical, or similar purposes.

Homochronous—The relationship between two signals such that their corresponding significant instants are displaced by a constant interval of time.

Hop—In radio communications, the excursion of a radio wave from the earth to the ionosphere and back to the earth. The number of hops indicates the number of reflections from the ionosphere.

Host—Any computer on a network that is a repository for services available to other computers on the network.

Hot Standby—In reliability, a method of hardware backup where the back-up equipment is under power and is (generally automatically) switched into the system when the primary operating equipment experiences a failure.

Human Factors Engineering (HFE)—An approach that makes use of scientific facts in the design of items (that is, computer systems, software, and so forth) to produce effective human-machine integration and utilization.

Human-Computer Interface (HCI)—HCI encompasses interactions between the user and the system, including controls, displays, environmental concerns, workspace layout, procedures, and documentation. HCI encompasses the look and feel of the interface, physical interaction devices, graphical interaction objects, alternate interactions (voice, touch screen, pen) environmental factors, and any other human-computer interactive methodology.

Hybrid—In communications-electronics, a functional unit in which two or more different technologies

are combined to satisfy a given requirement, combining the advantages of both into one system, such as an electronic circuit having both vacuum tubes and transistors, or a computer designed with both analog and digital characteristics.

Hybrid Coil—In telecommunications, an electrical device designed to convert between 2-wire and 4-wire circuits. Synonym: Hybrid Transformer, Bridge Transformer.

Hybrid Coupler—In an antenna system, a hybrid junction used as a directional coupler.

Hybrid Spread Spectrum—In radio communications, a combination of frequency hopping spread spectrum and direct-sequence spread spectrum.

Hyperlink—Pointers to other HTML documents. The hyperlink is actually a Uniform Resource Locator (URL) Internet address of the linked document.

Hypermedia—Computer-addressable documents that contain pointers for linking to multimedia information such as text, graphics, video, or audio in the same or other documents. NOTE: The use of hypertext links is known as navigating.

Hypertext—(1) The system of coding used to create or navigate hypermedia documents in a nonsequential manner. (2) Textual data stored in a network of nodes connected by links so that it can be accessed directly in a nonsequential manner. These links may reflect relationships not apparent on linear text. The operation of the World Wide Web relies mainly on hypertext as its means of interacting with users. Hypertext is basically the same as regular text with an important exception, it contains connections within the text to other documents.

HyperText Markup Language (HTML)—In electronic publishing, one of several markup languages that have evolved from the Standard Generalized Markup Language (SGML), primarily because of the Internet. It is the standard language the World Wide Web uses to create and recognize hypermedia documents. Web documents are typically written in HTML and are usually named with the suffix .htm.

HyperText Transfer Protocol (HTTP)—The protocol for moving hypertext files across the Internet. Requires an HTTP client program on one end, and an HTTP server program on the other end. The primary protocol used to communicate on the World Wide Web.

Icon—Graphical representation of an object, concept, or message used by a computer system to represent items such as files, documents, programs, and disk drives.

Identity Token—(1) Smart card, metal key, or other physical object used to authenticate identity. (2) Smart card, metal key, or some other physical token carried by a system's user allowing user identity validation.

Identity Validation—Tests enabling an communications and information system to authenticate users or resources.

Idle-Channel Noise—In telecommunications, random noise signals that are present in a communications channel when no intelligence signals are applied to it. The conditions and terminations must be stated for the noise measurements to be meaningful. Also see Noise.

Image—A picture stored on paper, as lines and characters on a video display tube, or as an electronic image encoded in magnetic or optical media.

Image Formation Time (IMF)—The time required to update screen image displays.

Image Frequency—In frequency heterodyning, an undesired input frequency that is capable of

producing the same output frequency (intermediate frequency) that the desired input frequency produces.

Imagery—Collectively, the representation of objects reproduced electronically or by optical means on film, electronic display devices, or other media.

Imitative Communications Deception—Introduction of deceptive messages or signals into an adversary's telecommunications signals.

Impedance—In electronics, the total opposition of an electronic circuit, device or component to the flow of an alternating current through the circuit, device, or component.

Implant—Electronic device or electronic equipment modification designed to gain unauthorized interception of information-bearing emanations.

Implementation—(1) Procedures governing the mobilization of the force and the deployment, employment, and sustainment of military operations in response to execution orders issued by the National Command Authorities. (2) The publication by the DoD components of directives, instructions, regulations, and related documents that define responsibilities and authorities and establish the internal management processes necessary to carry out the policies required by DoD issuances.

Impulse—A surge of electrical energy, usually of short duration and of a nonrepetitive nature.

Impulse Noise—Noise consisting of random occurrences of energy spikes, having random amplitudes and bandwidths; its presence in a data channel can be a prime cause of errors.

In-Band—In telecommunications, a method of sending management and/or control signals on the same frequency or within the same frequency band as that of the intelligence or data signals.

In-Band Signaling—In telecommunications, the transmission of signaling (ringing) information that uses frequencies or time slots that lie within the bandwidth of the information (normally voice) channel.

In-Circuit Emulator (ICE)—A combined hardware and software system that enables a prototype microprocessor system to be tested.

Inclined Orbit—The orbit of a satellite that is neither equatorial nor polar.

Independent Sideband Transmission—That method of double sideband transmission in which the information carried by each sideband is different (the carrier may be suppressed).

Indexing—The process used to identify a document, specific images, or data elements for retrieval purposes.

Information—(1) Facts, data, or instructions in any medium or form. (2) Any communications or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. (3) The meaning that a human assigns to data by means of the known conventions used in their representation. (JP1-02)

Information Appliance—A communications device which connects to the information utility to make information available to the user. Examples are: telephones, facsimile machines, desktop computers, network hubs, servers, etc.

Information Assurance (IA)—Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Attack—An activity taken to manipulate or destroy an adversary's information without visibly changing the physical entity within which it resides.

Information Bit—A bit that is generated by the data source and delivered to the data sink and which is not used by the data transmission system.

Information Combat—The employment of information warfare actions in support of military operations.

Information Dominance—(1) That degree of superiority in information functions that permit friendly forces to operate at a given time and place without prohibitive interference from opposing forces. (2) A condition in which a nation possesses a greater understanding of the strengths, weaknesses, interdependencies, and centers of gravity of an adversary's military, political, social, and economic infrastructure than the adversary has of that nation.

Information Engineering—(1) An integrated and evolutionary set of tasks and techniques that enhance business communication throughout an enterprise enabling it to develop people, procedures, and systems to achieve its vision. (2) A formal software engineering methodology that covers the complete information system life cycle from organization mission to application software and database development and maintenance.

Information Environment—The aggregate of individuals, organizations, or systems that collect, process, or disseminate information using any medium or form, including the information itself.

Information Flow—The movement of information from its source to the user, including all handling, processing, and transfers that enable its movement.

Information Flow Control—Procedure to ensure that information transfers within an communications and information system are not made from a higher security level object to an object of a lower security level.

Information Fusion—The process of reducing information to the minimum essentials and putting it in a form where it can be acted upon by those who need the information.

Information Grid—The networks that result from open systems architectures. Information grids refer to computer controlled networks that provide virtual connectivity on the demand of the warfighters. They support local and area network operations. They are also the basic components of larger network grids that, when interconnected, support regional, theater, and ultimately a global information grid.

Information Integrity—The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

Information Label—In Information Assurance, a piece of information that accurately and completely represents the sensitivity of the data in a subject or object.

Information Life Cycle—The stages through which information passes, typically characterized as creation or collection, processing, disseminating, use, storage, and disposition.

Information Management (IM)—The planning, budgeting, manipulating, and controlling of information throughout its life-cycle (e.g., creation or collection, processing, dissemination, use, storage, and disposition).

Information Model—(1) A term used to describe the information resources of the organization and their interrelationships. It is used to support data modeling and resulting database and document storage design

requirements. It provides the information resource managers' views of the architecture. (2) A model that represents the processes, entities, information flows, and elements of an organization and all relationships between these factors.

Information Munitions—In information warfare, software programs or logic elements designed to affect an adversary's information systems.

Information Operations (IO)—(1) Actions taken to affect adversary information and information systems while defending one's own information and information systems. (DoD) (2) Those actions taken to gain, exploit, defend or attack information and information systems and include both information-in-warfare and information warfare. (USAF)

Information Processing Equipment—Any electronic hardware used to process, transfer, or display data. Note, however, that radar and radio aids to navigation are not a function of this regulation.

Information Processing Services—A discrete set of personnel, information technology, and support equipment with the primary function of providing services to more than one agency on a reimbursable basis.

Information Processing Standards for Computers (IPSC)—A standardization area of the Defense Standardization Program. This area relates to computers and data processing devices, equipment and systems, including, but not limited to character recognition types, input/output media, formats and labels, programming language, computer documentation, flowcharts and terminology, character codes, data communications and input/output interfaces.

Information Protection—Measures to protect friendly information systems by preserving the availability, integrity, and confidentiality of the systems and the information contained within the systems.

Information Protection Operations—Proactive security functions established to assist Air Force organizations to deter, detect, isolate, contain, and recover from intrusions of computers and computer networks.

Information Protection Services Scalability—The ability to provide functionality up and down a graduated series of application platforms that differ in the speed and capacity, with out loss of functionality.

Information Protection Tools—Tools which perform numerous security functions including boundary protection, viral detection, intrusion detection, profile inspection, network mapping, remote patching, and on-line surveys.

Information Resources—Information and related resources, such as personnel, equipment, funds, and information technology.

Information Resources Management (IRM)—The process of managing information resources to accomplish agency missions and to improve agency performance, including through the reduction of information collection burden on the public. The term encompasses both information itself and the related resources such as personnel, equipment, funds, and information technology.

Information Security (INFOSEC)—The protection and defense of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security.

Information Services (ISvs)—(1) A discrete set of information activities typically provided on a reimbursable basis. These activities include analysis, acquisition, test, delivery, operation, or management of hardware, software, and communications systems. (DoD). (2) Information services include both actions taken and the resources to protect, manage, process, and exchange information for all secure and non-secure operations, command and control, and mission support functions. Specifically, Air Force information services are composed of interconnected communications and supporting information systems, including all logical and physical information assurance safeguards, that create a worldwide network to protect, manage, process, and exchange information. (AFDD 2-5)

Information Standards and Technology (INST)—A standardization area of the Defense Standardization Program. This area encompasses report standards, data exchange format standards, graphic, and imagery constructs. It includes the structure, values, definition, and representation of data that gives it meaning, enhances information sharing and exchange, and facilitates effective decision-making based on a DoD-wide commonality of representation and understanding of specific bits of information. Standard structures and formats include character and bit oriented syntax as well as graphics, imagery, and geographical constructs. These information structures are derived by combining and using standard data elements and codes to convey precise meaning.

Information Superiority (IS)—(1) The ability to obtain and transmit information unimpeded to any destination as and when needed and to exploit or deny an adversary's ability to do so. This includes the ability to manage information throughout its life-cycle, i.e., to create, collect, process, disseminate, use, store, and dispose of an unimpeded flow of information while exploiting or denying an adversary's ability to do the same. (DoD CIO) (2) The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (DODD S-3600.1) (3) That degree of dominance in the information domain which permits the conduct of operations without effective opposition. (JP 1-02) (4) ***NOTE:*** The Air Force prefers to cast "superiority" as a state of relative advantage, not a capability, and views IS as: That degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition. (AFDD 2-5)

Information System (IS)—(1) The means used to acquire, transform, store, or transmit information. (DoDD S-3600.1) (2) The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. (JP 1-02) (3) A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information Systems Security—The protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users or the provision of service to unauthorized users (includes those measures necessary to detect document, and counter such threats).

Information Systems Security Officer (ISSO)—Person responsible to the designated approving authority for ensuring the security of an information system throughout its life cycle, from design through disposal. Synonymous with Systems Security Officer.

Information Systems Security Product—Item (chip, module, assembly, or equipment), technique, product or service that performs or relates to information systems security.

Information Technology (IT)—(1) With respect to an executive agency, any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage

manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the DoD component. For purposes of the preceding sentence, equipment is used by a DoD component if the equipment is based by the DoD component directly or is used by a contractor under a contract with the executive agency which (a) requires the use of such equipment or contract, or (b) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. (2) The term "information technology" includes computers, ancillary equipment, software, firmware similar procedures, services (including support services), and related resources. (3) Notwithstanding definitions 1. and 2., IT does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. (DoDD 8000.1)

Information Technology System (ITS)—Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Information technology includes computers, ancillary equipment, software, firmware, and similar procedures; services (including support services), and related resources.

Information Technology System (ITS) Standards—Documents that provide technical definitions for information system processes, procedures, practices, operations, services, interfaces, connectivity, interoperability, information formats, information content, interchange, and transmission or transfer. Information technology standards apply during the development, testing, fielding, enhancement, and life-cycle maintenance of DoD information systems. Information technology standards include nongovernment national or international standards, federal standards, military standards, and multinational treaty organization standardization agreements. They may take numerous forms including standards, handbooks, manuals, specifications, commercial item descriptions, and standardized drawings, all are referred to collectively as Standards.

Information Utility—A provider of access to information services. To the customer the information utility is transparent and appears as an unrestricted transport of information from source to destination.

Information Warfare (IW)—(1) Information operations conducted during time of crises or conflict to achieve or promote specific objectives over a specific adversary or adversaries. (DODD S-3600.1). (2) Information operations conducted to defend one's own information and information systems, or to attack and affect an adversary's information and information systems (AFDD 2-5).

Information-based Processes—Processes that collect, analyze, and disseminate information using any medium or form. These processes may be stand-alone processes or sub-processes which, taken together, comprise a larger system or systems of processes. Information-based processes may be found in any facet of military operations, from combat through combat support and combat service support across the range of military operations.

Information-in-warfare (IIW)—Involves the Air Force's extensive capabilities to provide global awareness throughout the range of military operations based on integrated intelligence, surveillance and reconnaissance (ISR) assets; its information collection/dissemination activities; and its global navigation and positioning, weather, and communications capabilities.

Infostructure—The shared computers, ancillary equipment, software, firmware and similar procedures, services, people, and related resources used in the acquisition, storage, manipulation, protection, management, movement, control, display, switching, interchange, transmission, or reception of data or information in any format including audio, video, imagery, or data, whether supporting Information Technology (IT) or National Security systems as defined in the Clinger-Cohen Act of 1996.

Infra Low Frequency (ILF)—Frequencies of electromagnetic waves in the range of 300-3000 hertz.

Infrasonic Frequency—A frequency below that of sound waves audible to the human ear. Usually taken as a frequency of 15 hertz.

Infrastructure—(1) The term infrastructure is used with different contextual meanings. Infrastructure most generally refers to and has a hardware orientation, but is frequently more comprehensive and includes software and communications. Collectively, the structure must meet the performance requirements of and capacity for data and applications requirements. Just citing standards for designing an architecture or infrastructure does not include functional and mission area requirements for performance. Performance requirements metrics must be an inherent part of an overall infrastructure to provide performance interoperability and compatibility. It identifies the top-level design of communications, processing, and operating system software. It describes the performance characteristics needed to meet database and application requirements. It provides a geographic distribution of components to locations. The infrastructure architecture is defined by the service provider for these capabilities. It includes processors, operating systems, service software, and standards profiles that include network diagrams showing communications links with bandwidth, processor locations, and capacities to include hardware builds versus schedule and costs. (DoD). (2) At the national level, the framework of interdependent networks and systems, comprising identifiable industries, institutions, and distribution capabilities that provide a continual flow of goods and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, or society as a whole. (3) At the base level, the common-user portion of the communications and information systems environment. It includes transmission, switching, processing, system-control and network-management systems, equipment, and facilities that support the base. Examples are the telephone switch and cable plant, base communications center, land mobile radio system, and local area networks.

Infrastructure Asset—Any infrastructure facility, equipment, service, or resource that supports a DoD component. A critical infrastructure asset is an infrastructure asset deemed essential to DoD operations or the functioning of a critical asset.

Initial Distribution (ID)—The first automatic distribution of a new or revised publication, either by a publishing distribution center to a publishing distribution office (PDO), or by a PDO to a customer account representative, against established requirements, or direct to addresses designated by an office of primary responsibility.

Initial Operational Capability (IOC)—(1) At the system level, IOC is the point at which some portion of the technical and operational specifications defined by the requirements' documents have been achieved. The specific definition of IOC will vary for each system and would be negotiated between the program manager, the user, and the operations and maintenance (O&M) activity. (2) At the site level, IOC is the point at which the technical specifications of that portion of the system installed at a specific site meet the documented requirements, but some portion of testing and, or operational specifications remains to be accomplished. The specific definition of IOC is site specific and would be negotiated between the program manager, the site manager, and the O&M activity.

Initialize—Setting the state of a cryptographic logic prior to key generation, encryption, or other operating mode.

In-Line Image—In networking, a graphic image that is displayed with an hypertext mark-up language (HTML) document.

In-Phase—In electronics, pertaining to signals that have zero (voltage or current) phase shift relative to

each other. In-phase signals, when combined, generally result in a stronger signal. Compare out-of-phase.

In-Plant System—Synonymous with In-House System.

Input—Data or signals keyboarded or transmitted into a computer system.

Input/Output Channel—A device that handles the transfer of data between internal memory and peripheral equipment.

Input/Output Device—A device that introduces data into or extracts data from a system.

Inquiry—A request for information from storage (a request for specific information from a stored collection of data).

Inside Plant—All the cabling and equipment installed in a telecommunications facility.

Inside-the-Gate—Collective term for the various components that make up the base communications infrastructure, consisting primarily of the Network Control Center, on-base cabling, and transmission systems.

Inspectable Space—Three dimensional space surrounding equipment that process classified and/or sensitive information within which TEMPEST exploitation is not considered practical or where legal authority to identify and/or remove a potential TEMPEST exploitation exists. Synonymous with Zone Control.

Institute of Electrical and Electronics Engineers (IEEE)—An accredited standards body that has produced standards such as the network-oriented 802 protocols and portable operating system interface for computer environment (POSIX). Members represent an international cross-section of users, vendors, and engineering professionals.

Instrument Landing System (ILS)—(1) A system of radio navigation intended to assist aircraft in landing which provides lateral and vertical guidance, which may include indications of distance from the optimum point of landing. (2) A radio navigation system that provides aircraft with horizontal and vertical guidance just before and during landing and, at certain fixed points, indicates the distance to the reference point of landing.

Instrument Landing System (ILS) Glide Path—A system of vertical guidance embodied in the ILS that indicates the vertical deviation of the aircraft from its optimum path of descent.

Instrument Landing System (ILS) Localizer—A system of horizontal guidance embodies in the ILS that indicates the horizontal deviation of the aircraft from its optimum path of descent along the axis of the runway.

Integrated Circuit (IC)—In electronics, a combination of interconnected circuit elements inseparable associated on or within a continuous substrate. An IC may contain from a few to many thousands of transistors, resistors, capacitors, and diodes.

Integrated Computing—In programming, the concurrent use of data by two or more software packages (for example, a graphics package that displays spreadsheet data).

Integrated Database—A database of logically integrated entities, relationships, and attributes created after analysis of an information model.

Integrated Drive Electronics (IDE)—In computers, a standard electronic interface used between the computer's motherboard's data paths and the computer's storage devices (e.g., hard drive, diskette drive,

etc.).

Integrated Optical Circuit—In opto-electronics, the optical equivalent of a microelectronic circuit.

Integrated Services Digital Network (ISDN)—A system of digital phone connections which allows voice and data signals to be carried simultaneously over a standard analog telephone line between the local telephone central office and the customer equipment. Special equipment is needed to communicate with the telephone company's switch and with other ISDN devices, such as terminal adapters and routers. Basic ISDN service provides two channels which can each carry 64 kbps of data or a voice call, or can be combined to provide a single 128 kbps channel.

Integrated System—A telecommunications system that transfers analog and digital traffic over the same switched network.

Integration—In communications, the arrangement of systems in architecture so that they can function together in an efficient and logical way.

Integration Framework—In the context of the Air Force portal, an information system's organizational structure that willl enable many information systems to interface within a single information backbone at several different levels of integration.

Integrity—(1) In data communications, absolute verification that data has not been modified in transmission or during computer processing. (2) Quality of an information system that reflects the logical correctness and reliability of the operating system; the logical completeness of the hardware and software that implement the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. In a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

Integrity Check Value—Checksum capable of detecting modification of an information system.

Intelligent Terminal—A terminal containing a microprocessor and is capable of emulating other terminals, validating data, implementing protocols, and so forth.

Interactive Process—A process of calculating a desired result by a repeating cycle of operations that comes closer and closer to the desired result; conversational operation of a computer system using an on-line cathode ray tube terminal.

Interactive Service—In an integrated services digital network, a telecommunications service that facilitates a bi-directional exchange of information among users or among users and hosts. Interactive services are grouped into conversational services, messaging services, and retrieval services.

Interactive Video Disk (IVD)—A desktop, computer-based training system combining an optical laser disk player, microcomputer, and a television monitor. The interaction is achieved by using a touch screen, lightpen, keyboard, or other input device. The user's interactivity is achieved through an operating program specifically designed and authored for each IVD course.

Interactive—Computer programs that allow performance of several complex functions or operations at the same time, based on response from the operator.

Interconnection—The linking together of interoperable systems.

Interface Control Document—Technical document that describes interface controls and identifies the authorities and responsibilities for ensuring the operation of such controls. This document is baselined during the preliminary design review and is maintained throughout the information system life cycle.

Interface—(1) A boundary or point common to two or more similar or dissimilar communications systems, subsystems, or other entities against which or at which necessary information flow takes place. (2) A concept involving the specification of the interconnection between two systems or items of equipment. The definition includes the type, quantity, and function of the interconnecting circuits and the type and form of signals to be interchanged via those circuits. Mechanical details of plugs, sockets, pin numbers, and so forth, may be included within the context of the definition. (3) The process of interrelating two or more dissimilar circuits or systems. (4) A connecting link between two systems. In the open system interconnection reference model, it is the boundary between adjacent layers. (5) Common boundary between independent systems or modules where interactions take place.

Interference—The effect of unwanted energy due to one or a combination of emissions, radiation, or inductions on reception in a radio communications system, manifested by any loss of information that could be extracted in the absence of such unwanted energy.

Interim Approval—Temporary authorization granted by a designated approving authority for an information system to process information based on preliminary results of a security evaluation of the system.

Interim Contractor Support (ICS)—A preplanned, temporary logistics support alternative for the initial period of operational use of a new or modified system for which eventual organic support is planned.

Interleaving—(1) In digital communications, the transmission of pulses from two or more digital sources in time division sequence over a single path. (2) A technique used in conjunction with error correcting codes to lower the error rates of communications channels characterized by burst errors.

Interlock—To arrange controls of machines or devices so that their operation is interdependent in order to ensure their proper coordination.

Intermediate Language—A language other than machine code that is produced by a compiler as a step in compiling a high-level language program.

Intermodulation—In communication-electronics, the production, in a nonlinear transducer element, of frequencies corresponding to the sums and differences of the fundamentals and harmonics of two or more frequencies which are transmitted through the transducer.

Intermodulation Noise—In a telecommunications transmission path or device, (undesirable) noise that is generated during modulation and demodulation and is the result of nonlinear characteristics in the path or device.

Internal Information Collection/Reporting Requirement—Data or information collected by one or more organizational components and transmitted to other organizational components for management purposes. The collections required for management purposes pertain to policy; planning, controlling, and evaluating operations and performance; making administrative determinations; and preparing other reports. It is status, summary, or statistical information in both electronic and manual information systems.

International Organization for Standards (ISO)—An international organization responsible for the development and publication of international standards in various technical fields. It consists of member bodies that are the national standards bodies of most of the countries of the world. The ISO has its headquarters in Geneva, Switzerland. The American National Standards Institute is the representative standards body for the United States.

International Standards (IS)—Agreed upon international standards as voted by the International Organization for Standards. (See ISO).

International Telecommunication Union (ITU)—Formerly, the International Telegraph and Telephone Consultative Committee (CCITT). The ITU, with headquarters in Geneva, Switzerland, is an international organization within which governments and the private sector coordinate global telecommunication networks and services. Activities include telecommunications standardization, radio communications, telecommunications development, and organization of telecommunications events. The ITU promotes standardized telecommunications on a worldwide basis. It is recognized by the United Nations Organization as the specialized agency for telecommunications.

Internet—A catch-all term used to describe the massive worldwide network of computers. Literally, it means network of networks and is a worldwide interconnection of individual networks operated by government, industry, academia, and private sectors. Although there is no single governing body that controls the internet, there are companies that help manage different parts of the networks that tie everything together. The networks within different countries are funded and managed locally according to local policies. Access to the internet means access to a number of basic services, such as electronic mail, interactive conferences, access to information resources, network news, and files transfer capability.

Internet Standard—A standard produced by the Internet Architecture Board that identifies one or more internet requests for comment that are required for a given data communications function or internet service.

Internetwork Private Line Interface—Network cryptographic unit that provides secure connections, singularly or in simultaneous multiple connections, between a host and a predetermined set of corresponding hosts.

Interoperability Standard—A document that establishes engineering and technical requirements that are necessary to be employed in the design of systems, units, or forces, and to use the services so exchanged to enable them to operate effectively together.

Interoperability—(1) The ability of systems, units, or forces to provide services to and accepts services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. (2) The condition achieved among communications-electronics systems or equipment when information or services can be exchanged directly and satisfactorily between them and, or their users.

Interrupt—A break in the normal flow of a system or routine such that flow can be resumed from that point at a later time.

Intramodal Distortion—In an optical fiber, distortion caused by dispersion, such as material or profile dispersion, of a given propagating mode.

Intranet—(1) A private access network that functions like the Internet, but is not part of it. Usually owned and managed by an organization, an intranet enables an activity to share its resources with its members without making sensitive information available to users with Internet access. Intranets may allow connectivity with the Internet through firewall servers and other security measures to maintain its internal security. (2) A private network inside a company or organization that uses the same kinds of software as found on the internet, but that is only for internal use.

Intrinsic Noise—In telecommunications, in a transmission path or device, that noise which is inherent to the path or device and is not contingent upon modulation.

Intrinsically Safe (IS)—The National Electrical Code defines IS equipment as equipment not capable of releasing sufficient electrical or thermal energy to cause ignition of specific flammable or combustible atmospheric mixture in its most ignitable concentration.

Inward-Outward Dialing—A dialing capability where calls are dialed directly to and from base telephone stations without operator assistance. Inward-outward dialing improves speed of service, reduces switchboard operator workload, and lowers operating costs.

Ionosphere—That part of the earth's atmosphere, extending from approximately 70 kilometers to 500 kilometers altitude, where ions and free electrons exist in sufficient quantities to reflect electromagnetic waves.

Ionosphere Sounder—A device that transmits signals to determine the degree of usability of the ionosphere for radio transmissions.

Ionospheric Scatter—The propagation of radio waves by scattering due to irregularities or discontinuities in the ionization of the ionosphere. Synonym: Forward Propagation Ionospheric Scatter.

IP Perspective—A philosophy where all security disciplines are coupled together with COMPUSEC to provide complete security for sensitive and classified information. In order to provide realistic and effective security for a system, certification must include all appropriate security disciplines.

Isochronous—In communications-electronics, that characteristic of a periodic signal in which the time interval separating any two corresponding transitions is theoretically equal to the unit interval or to a multiple of the unit interval. Pertaining to data transmission in which corresponding significant instants of two or more sequential signals have a constant phase relationship.

Isotropic Antenna—A hypothetical antenna that radiates or receives equally in all directions. Isotropic antennas do not exist physically, but represent a convenient reference for expressing directional properties of actual antennas.

Jabber Control—In data communications, a facility in a local area network to interrupt automatically transmission of an abnormally long-output data stream.

Jitter—(1) In communication-electronics, abrupt and spurious variations in a signal, such as in interval duration, amplitude of successive cycles, or in the frequency or phase of successive pulses. When used qualitatively, the term must be identified as being time, amplitude, frequency, or phase related and the form must be specified. When used quantitatively, a measure of the time or amplitude related variation must be included (for example, average, root-mean-square, peak-to-peak, and so forth). (2) In computer graphics, a signal instability resulting in sudden, small, irregular variations due mainly to synchronizing defects in the associated equipment. (3) In facsimile, raggedness in the received copy caused by erroneous displacement of recorded spots in the direction of scanning.

Job Control Language (JCL)—In computing, a problem-oriented language used for specifying the environment for running a particular batch of work.

Job-Oriented Terminal—In peripherals, a terminal designed for a particular application.

Joint Communications Control Center (JCCC)—An activity at the unified or joint command headquarters with primary responsibility for overall C4 systems management.

Joint Doctrine—Fundamental principles that guide the employment of forces of two or more services in coordinated action toward a common objective. It will be promulgated by the Chairman, Joint Chiefs of

Staff, in consultation with the other members of the Joint Chiefs of Staff.

Joint Interface—An interface that passes or is used to pass information between systems or equipment operated by two or more commanders in chief, services, and, or agencies.

Joint Photographic Experts Group (JPEG)—A compression method of storing an image in digital format.

Joint Publications—Publications of joint interest prepared under the cognizance of Joint Staff directorates and applicable to the military departments, combatant commands, and other authorized agencies. It is approved by the Chairman, Joint Chiefs of Staff, authenticated by the Director of the Joint Staff, and distributed through service channels.

Joint Tactical Information Distribution System (JTIDS)—An information distribution system that provides secure integrated communications, navigation, and identification capability for application to military tactical operations. A proposed version of a joint doctrine or joint tactics, techniques, and procedures publication that normally contains contentious issues and is nominated for a test publication and evaluation stage.

Joint Technical Architecture (JTA)—(1) The JTA identifies a common set of mandatory information technology standards and guidelines to be used in all new and upgraded Command, Control, Communications, Computers, and Intelligence (C4I) acquisitions across the Department of Defense (DoD). (2) The DoD JTA provides DoD systems with the basis for the needed seamless interoperability. The JTA defines the service areas, interfaces, and standards (JTA elements) applicable to all DoD systems; its adoption is mandated for the management, development, and acquisition of new or improved systems throughout the DoD.

Joint Test Publication (JTP)—A draft of a joint doctrine or joint tactics, techniques, and procedures that has evolved far enough in development to be approved for evaluation by the Director, Operational Plans and Interoperability (J-7), Joint Staff. Publication of a test publication does not constitute Chairman, Joint Chiefs of Staff, approval of the publication. Prior to final approval as joint doctrine, test publications are expected to be further refined based upon evaluation results.

Joint Universal Data Interpreter (JUDI)—An integrated software system that provides a fused tactical display of component forces executing on any platform. JUDI is a translator that interprets data formats, parses and analyzes the data, stores the data in a universal database, and then formulates the messages for output. It provides interoperability among some major existing command and control systems without the need to modify those systems.

Joint Worldwide Intelligence Communications System (JWICS)—(1) The Sensitive Compartmented Information (SCI) portion of the Defense Information System Network. It incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing. (2) A high speed (T-1, 1.544 Mbps) communications system designed to provide secure, system high (Top Secret/SCI) data, interactive video teleconferencing, and video broadcasting capabilities to its subscribers.

Journal—(1) In communications, a list of all messages sent and received by a terminal. (2) In computing, a chronological record of changes made to a set of data, often used for reconstructing a previous version of the set in the event of corruption.

Judder—In facsimile, an irregular movement of the moving parts in a transmitter or receiver causing straight lines in the source document to be reproduced in a wavy manner.

Jumper—(1) In electronics, a short wire used for the (normally temporary) connection of two points in an electric circuit. (2) A hardware link made within a circuit to select a particular option.

Junction—In electronics, the boundary region between two semiconductors having different electrical properties, or between a metal and a semiconductor. This boundary region is used to control the current flow through a semiconductor.

Justify—In composition, to space out lines of text so that they are of equal length.

K band—In radio communications, the frequency band between 18-27 GHz.

Ka band—In radio communications, the frequency band between 27-40 Ghz.

Kernel—(1) The essential central circuitry that is required to enable a microprocessor to operate (for example, power supply, the microprocessor itself, clock circuit). (2) A module of a program that forms a logical entity or performs a unit function.

Key—In cryptography, information (usually a sequence of random binary digits) used initially to set up and periodically change the operations performed in cryptoequipment for encrypting or decrypting electronic signals, for determining electronic counter countermeasures, or for producing other keys.

Key Card (CFD)—Paper card, containing a pattern of punched holes, that establishes key for a specific cryptonet at a specific time.

Key Distribution Center (KDC)—COMSEC facility that generates and distributes key in electrical form.

Key List—Printed series of key settings for a specific cryptonet. Key lists may be produced in list, pad, or printed tape format.

Key Management—Supervision and control of the process whereby key is generated, stored, protected, transferred, loaded, used, and destroyed.

Key Pair—Public key and its corresponding private key as used in public key cryptography.

Key performance Parameters (KPPs)—Those capabilities or characteristics considered essential for successful mission accomplishment. Failure to meet an Operational Requirements Document's (ORD) KPP threshold can be cause for the concept or system selection to be reevaluated or the program to be reassessed or terminated.

Key Production Key—Key used to initialize a keystream generator for the production of other electronically generated key.

Key Pulsing—A system of sending telephone calling signals in which the digits are transmitted by operation of a push-button key set. The type of key pulsing commonly used is dual-tone multi-frequency signaling; each push button causes generation of a unique pair of tones.

Key Storage Device (KSD)—A small device, shaped like a physical key which contains passive memory. It is used as a fill device and also as a crypto-ignition key (CIK) for a type I STU-III terminal.

Key Stream—Sequence of symbols (or their electrical or mechanical equivalents) produced in a machine or auto-manual cryptosystem to combine with plain text to produce cipher text, control transmission security processes, or produce key.

Key Tag—Identification information associated with certain types of electronic key.

Key Tape—Punched or magnetic tape containing key. Printed key in tape form is referred to as a key list.

Key Telephone System—In a local environment, terminals and equipment that provide immediate access from all the terminals to a variety of telephone services without attendant assistance.

Key Updating—Irreversible cryptographic process for modifying key.

Key-Auto-Key—Cryptographic logic that uses previous key to produce key.

Key-Encryption-Key (KEK)—Key that encrypts or decrypts other keys for transmission or storage.

Keying Material—Key, code, or authentication information in physical or magnetic form.

Keystone Equipment—Includes manufacturing, inspection, or test equipment and is the required equipment for the effective application of technical information and knowledge. Keystone materials have the same significant application.

Key—Usually a sequence of random or pseudo-random bits used initially to set up and periodically change the operations performed in cryptoequipment for the purpose of encrypting or decrypting electronic signals, or for determining electronic counter-countermeasures patterns (e.g., frequency hopping or spread spectrum), or for producing other key.

Kilo (k)—A prefix denoting one thousand (10^3).

Kilobytes (kb)—One kilobyte equals 1,024 bytes.

Kilohertz (kHz)—A unit of frequency denoting one thousand (10^3) hertz.

Knife-Edge Effect—The transmission of radio signals into the line-of-sight shadow region caused by the diffraction over an obstacle (for example, a sharply defined mountain top or ridge).

Knowledge—Understanding gained through experience, observation, or study.

Knowledge Management—The process through which an organization uses its collective intellectual capital to accomplish its strategic objectives.

Ku band—In radio communications, the frequency band between 12-18 GHz.

L—In publishing , a term meaning Limited Distribution.

L band—In radio communications, the frequency band between 1-2 GHz.

Labeled Security Protection (Class B1)—Elementary-level mandatory access control protection features and intermediate-level discretionary access control features in a trusted computing base that use sensitivity labels to make access control decisions.

Land Line—A colloquial name for conventional telephone services. Land lines include conventional twisted-pair lines, carrier facilities, and microwave radio facilities for supporting a conventional telephone channel, but do not include satellite links or mobile telephone links using radio transmissions.

Land Mobile Radio (LMR)—A radio used to provide local transfer of information by portable, mobile, or base station radios and associated equipment. LMRs include combat deployable radios and base support radios. Radio networks are established on the basis of functional agencies and usually have no connectivity between nets unless more than one net shares a frequency. Each net has its own radio system, antenna, code words, and call signs. The capability does exist for commercial encryption, but this system provides only privacy and not security.

Land Mobile Station—A mobile station in the land mobile radio service capable of surface movement within the geographical limits of an area, country, or continent.

Land Station—A station in the mobile radio service not intended to be used while in motion.

Language—In programming and communications, a set of characters, conventions, and rules used to convey information.

Language Processor—In programming, a computer or other functional unit for processing programs written in a specified programming language.

Lapse Rate—The magnitude of the decrease of an atmospheric parameter (temperature, pressure, of moisture). For example, the standard temperature lapse rate in the lower atmosphere is 2.0 degrees Celsius per 1,000 feet.

Laser—Abbreviation meaning light amplification by stimulated emission of radiation. In opto-electronics, a device that emits light rays that are in phase, traveling in the same direction, and essentially of the same wavelength (color). A laser beam does not diverge by a significant amount and maintains a high energy density.

Layer—In telecommunications networks and open system architecture, a group of related functions that are performed in a given level in a hierarchy of groups of related functions.

L-Band—In radio communications, the frequency range of 1-2 GHz.

Lead Command (LC)—Abbreviation for Lead Operating Command. In communications systems acquisition program management, the organization (MAJCOM, Direct Reporting Unit (DRU) or Field Operating Agency (FOA) designated as the Air Force advocate for all users (using commands) of a communications system, equipment, commodity, or service. Advocacy involves planning, programming, budgeting, and life-cycle management of the system.

Least Privilege—Principle requiring that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use of an information system.

Least Significant Bit (LSB)—In data structures, the bit that occupies the rightmost position in a binary number.

Least Significant Digit (LSD)—Same as Least Significant Bit.

Legacy Environments—Legacy environments could be called legacy architectures or infrastructures and, as a minimum, consist of a hardware platform and an operating system. Legacy environments are systems identified for phase-out, upgrade, or replacement. All data and applications software that operate in a legacy environment must be categorized for phase-out, upgrade, or replacement.

Legacy System—(1) A system that is a candidate for phase-out, upgrade, or replacement. Generally, legacy systems are in this category because they do not meet current standards. Legacy system workloads must be converted, transitioned, or phase out (eliminated). (2) A communications and information system that duplicates the support services provided by the migration system. Legacy systems must be terminated so that all future development and modernization can be applied to the migration system.

Level of Openness—The level (system, subsystem, or component) at which interfaces conform to open standards. The level of openness determines the extent to which a system can use multiple suppliers, insert new technology, and assign control on design, interfaces, repair, and implementation to the

contractor/supplier.

Level Of Protection—Extent to which protective measures, techniques, and procedures must be applied to information systems and networks based on risk, threat, vulnerability, system interconnectivity considerations, and information assurance needs. Levels of protection are: (1) Basic: information system and networks requiring implementation of standard minimum security countermeasures. (2) Medium: information system and networks requiring layering of additional safeguards above the standard minimum security countermeasures. (3) High: information system and networks requiring the most stringent protection and rigorous security countermeasures.

Life Cycle—(1) The period of time that begins when a (communications) system is conceived and ends when the system is no longer available for use. Life cycle is defined within the context of life cycle management in various DoD publications; it generally refers to the usable system life. (2) All phases of the system's life including research, development, test and evaluation, production, deployment, operations and support, and disposal.

Life-Cycle Cost—The total cost to the government for a system over its full life including the cost of development, procurement, operation, support, and disposal.

Life-Cycle Management—A management process, applied throughout the life of a system, that bases all programmatic decisions on the anticipated mission-related and economic benefits derived over the life of the system.

Light Emitting Diode (LED) Printer—A device similar in operation to a laser printer, except instead of a moving laser beam it uses light from an array of light-emitting diodes. This device has the advantage of having fewer moving parts than the laser printer.

Light Emitting Diode (LED)—In electronics, a semiconductor diode that glows when supplied with a specified voltage. LEDs are commonly used as alphanumeric display devices.

Light Pen—In peripherals, a light-sensitive device that is shaped like a pen and connected to a visual display unit. The tip of the light pen contains a light-sensitive element which, when placed against the screen, reacts to the presence of a scanning spot of the raster display which enables the computer to identify the location of the pen on the screen.

Line—In communications, a device for transferring electrical energy from one point to another, such as a transmission line or a communications channel.

Line Access Protocol (LAP)—In data communications, a data link layer protocol that is a subset of high-level data link control and is used in X.25-based networks.

Line Driver—A digital amplifier used to enhance transmission reliability over extended distances.

Line-of-Sight (LOS) Propagation—Radio propagation in the atmosphere which is similar to light transmissions in that the radio waves in the very high frequency and above ranges tend to travel as a beam in a straight line between the transmitting and receiving antennas. The intensity of the radio beam decreases mainly due to energy spreading according to the inverse-distance law. A line-of-sight path does not follow the curvature of the earth.

Line Replaceable Unit (LRU)—A module, subassembly, or printed circuit card within or attached to an item of communications equipment or computer, which can be replaced without soldering.

Line Transient—In communications, an unwanted voltage pulse of very short duration, which can often

produce errors in digital circuits that are not designed to minimize the effects of such interference.

Linear (Device)—In electronics, a device (amplifier, receiver) that produces an output signal that bears a linear relationship to the input signal.

Link Encryption—Encryption of information between nodes of a communications system.

Link Orderwire—A voice or data communications circuit that (a) serves as a transmission link between communications facilities interconnected by a transmission link, and (b) is used for coordination and control of link and traffic activities.

Link—(1) A general term used to indicate the existence of communications facilities between two points. (2) A portion of a circuit designed to be connected in tandem with other portions. (3) A radio path between two points (radio link). The term link should be defined or qualified when used. It is generally accepted that the signals at each end of the link are in the same form.

Liquid Crystal Display (LCD) Screen—A form of flat-screen visual display unit employing liquid crystal displays. It is lighter and much flatter than a cathode ray tube type display, requires very little electrical power to operate, and generates very little heat.

Liquid Crystal Display (LCD)—A display manufactured from two glass plates sandwiched together with a special fluid. When a voltage is applied, the light polarization in the liquid changes and the image becomes visible through a polarizing filter.

List-Oriented—Computer protection in which each protected object has a list of all subjects authorized to access it. See also Ticket-Oriented.

Load—(1) To fill the internal storage of a computer with information from auxiliary or external storage. (2) The (electrical) power consumed by a device or circuit in performing its function. (3) An power-consuming device connected to an electrical circuit.

Lobe—In radio communications, (1) An identifiable segment of an antenna radiation pattern; a lobe is characterized by a localized maximum signal strength bounded by identifiable nulls. (2) The formation of maxima and minima of signal strength at various angles of the main antenna beam caused by the reflection of energy from the ground or water surface and/or objects near the antenna. These reflections reinforce the main beam at some angles and detract from it at other angles producing lobes and nulls.

Local Area Network (LAN)—A telecommunications system, usually within a specified geographical area, designed to allow a number of independent devices to communicate with each other over a common transmission topology. LANs are usually restricted to relatively small geographical areas, such as rooms, buildings or clusters of buildings, and utilize fairly high data rates. Depending on the implementation, these communications networks can provide internal interchange of voice, data, graphics, video, or other forms of electronic messaging.

Local Authority—Organization responsible for generating and signing user certificates.

Local Management Device/Key Processor (LMD/KP)—An electronic key management system (EKMS) platform that provides automated management of COMSEC material and generates key for designated users.

Local Multipoint Distribution Service (LMDS)—A two-way, wireless, broadband technology which allows deployment of large amounts of bandwidth and a wide range of services to homes and businesses in the crucial "last mile" where bandwidth bottlenecks are most acute. Service applications include

high-speed Internet access, real-time multi-media file transfer, interactive video, video-on-demand, and telephony.

Local Reproduction Authorized (LRA)—A form that is reproduced locally. Stock is not available from the order sources.

Log Periodic Antenna—A broadband, multi-element, unidirectional, narrow-beam antenna whose frequency response characteristics are repeated at equally spaced frequencies, with the period equal to the logarithm of the ratio that determines the length and spacing of the elements.

Logic Bomb—A resident computer program that triggers the perpetration of an unauthorized act when particular states of the system are realized.

Logical Completeness Measure—Means for assessing the effectiveness and degree to which a set of security and access control mechanisms meets security specifications.

Logical Data Model—A model of data, derived from the functional model, used to develop databases and software solutions.

Logistics Support—(1) Logistics support encompasses the logistic services, materiel, and transportation required to support the continental United States-based and worldwide deployed forces. (2) The composite of all considerations necessary to assure the effective and economical support of a system throughout its programmed life cycle. Included are: supply support, maintenance planning, test and support equipment, transportation and handling, personnel and training, facilities, data and software.

Long-Haul Information Transfer—Information transfer elements that provide for inter-base and both intra- and inter-theater information flow between gateways to other information transfer components; information systems organizations control these resources.

Long-Haul Telecommunications—Communications that permit users to convey information on a worldwide basis. Compared to tactical communications, long-haul communications are generally characterized by higher levels of users (including National Command Authorities), more stringent performance requirements (higher quality circuits), longer distances between users (up to global distances), higher traffic volume and density (larger sizing of switches and trunk cross sections), and fixed or recoverable assets. Normally used in reference to the Defense Information System Network.

Loop—(1) The go and return conductors of an electric circuit; a closed circuit. (2) In computer systems, the repeated execution of a series of instruction for a fixed number of times. (3) In telephone systems, a pair of wires from a central office to the subscriber's telephone.

Loop Test—A test that uses a closed circuit (that is, loop), to detect and locate faults.

Loss—(1) The amount of electrical attenuation in a circuit, or the power consumed in a circuit or component. (2) The energy dissipated without accomplishing useful work, usually expressed in decibels.

Low Data Rate (LDR)—Data rates between 75 bps and 19,200 bps.

Low-Delay Codebook Excited Linear Predictive (LD-CELP)—In Voice over Internet Protocol (VoIP), a speech compression method that provides near toll quality audio by using a smaller sample size that is processed faster, resulting in lower delays.

Low Frequency (LF)—Frequencies of electromagnetic waves in the range of 30-300 KHz.

Low Level Language—A language designed to facilitate the writing of efficient programs that execute rapidly with minimum main storage space. They are designed for programming computers of particular

makes and models. A low level language may also be termed a computer-oriented language.

Low Level Protocol—In data communications, a protocol that is concerned with the mechanics of communication within a network.

Low Pass Filter—In electronics, a frequency-selective network that attenuates signals with frequencies above a predefined value, but passes signals with lower frequencies.

Low-Noise Amplifier (LNA)—In communications-electronics, an amplifier designed to minimize the noise introduced in the early stages of amplification, especially where very weak incoming signals are concerned. An LNA is generally used as the first stage of amplification in most wideband radio receiver systems.

Machine Cryptosystem—A cryptosystem in which cryptographic processes are performed by cryptoequipment.

Machine Instruction—An instruction that is written in a machine language and can be executed directly by the processor for which it was designed without translation or interpretation.

Machine Language—In programming, a language for programs that can be expressed directly in binary format acceptable to the central processing unit (CPU). All other programming languages (low- or high-level languages) have to be translated into binary machine code before being executed in the CPU.

Machine Readable—Instructions coded so a computer can understand and process them without further intervention.

Macro—In programming, a pre-defined and recorded series of keystrokes that are used later to simplify repetitive tasks.

Macro Language—In programming, the representations and rules for writing macro-instructions.

Macrobend Loss—In fiber optics, the leakage of light caused by a bend in the cable.

Magnetic Core—A configuration of magnetic material that is intended to be placed in a certain relationship to electric currents and whose magnetic properties are essential to its use.

Magnetic Media—The physical substances used by a computer system (analog or digital) upon which data is recorded through the use of magnetic fields.

Mail Control Activity—A civilian or military facility established to oversee the handling of military mail at international and military airports.

Main Distribution Frame (MDF)—The cable racking in a telecommunications facility on which all distribution and trunk cables into a central office are terminated. (The bulky processing units of the early computers resembled the MDF, hence the origin of the term mainframe for a large computer.)

Main Lobe—Of an antenna radiation pattern, the lobe containing the maximum power, typically the central lobe.

Main Memory—In memory systems, a program addressable, random access store that transfers instructions/data to and from the central processing unit. The main memory also transfers data to and from backing storage and peripherals.

Mainframe—In computing, a term normally applied to a large, general-purpose computer installation serving a major section of an organization or institution.

Maintainability—A characteristic of design and installation that is expressed as the probability that an item will be retained in or restored to a specific condition within a given period of time, when the maintenance is performed in accordance with prescribed procedures and resources.

Maintenance Concept—A primary factor in determining logistics support requirements for a (C4) system. It delineates maintenance support levels, maintenance responsibilities (organic and/or contractor), supply responsiveness factors, facility utilization requirements, and maintenance environments.

Maintenance Engineering—The application of techniques, engineering skills, and effort, organized to ensure that the design and development of weapon systems and equipment provide adequately for their effective and economical maintenance.

Maintenance Planning—A process that includes all planning and analysis associated with the establishment of requirements for overall support of a (C4) system throughout its life cycle. It begins with the development of a maintenance concept, continues through the accomplishment of logistics support analysis during the design and development phases, procurement, acquisition of support items, and through the customer use phase when an ongoing system capability is required to sustain operations.

Maintenance—The function of keeping a (communications) system in, or restoring it to, serviceable condition. Maintenance is not intended to increase the value, capabilities, or expected life of a system, but to keep it in efficient operating condition. Equipment/system maintenance includes servicing, repair, modification, modernization, overhaul, inspection, condition determination, corrosion control, and initial provisioning of support items. Maintenance includes both preventive and corrective actions. Maintenance of software includes anticipating, detecting, and eliminating errors.

Maintenance Concept—A brief description of maintenance considerations, constraints, and plans for operational support of the system/equipment under development.

Malicious Logic—Hardware, software, or firmware that is intentionally included into an information system for an unauthorized purpose (e.g., virus).

Mandatory Access Control (MAC)—Means of restricting access to objects based on the sensitivity of the information contained in the objects and the formal authorization (i.e., clearance, formal access approvals, and need to know) of subjects to access information of such sensitivity. See Discretionary Access Control.

Manual Remote Rekeying—Procedure by which a distant cryptoequipment is rekeyed electrically, with specific actions required by the receiving terminal operator.

Mapping—The electronic process of creating the edits, rules, and algorithms that control the data entry processing for electronic forms.

Marker Beacon—A radio transmitter in the aeronautical radio navigation service that vertically radiates a distinctive pattern to provide position information to aircraft.

Masquerading—A form of spoofing.

Master Crypto-Ignition Key (CIK)—A key device with electronic logic and circuits, providing the capability for adding more operational CIKs to a keyset (maximum of seven) any time after fill procedure is completed. The master CIK can only be made during the fill procedure as the first CIK.

Master File—The definitive version of a data file in an automated system. The file is long-term, even though the data may change.

Maximum Usable Frequency (MUF)—The upper limit of the frequencies that can be used at a specific time for radio transmission between two points and involving propagation by reflection from the regular ionized layers of the ionosphere.

Meaconing, Intrusion, Jamming, and Interference (MIJI)—Meaconing, intrusion, and jamming are areas of electromagnetic energy transmission classified as intentional or deliberate action by unfriendly nations. Specifically, meaconing is the transmission or retransmission of actual or simulated signals to confuse radio navigation. Intrusion is the intentional insertion of electromagnetic energy into signal transmission paths, with the objective of deceiving operators or causing confusion. Jamming is the deliberate radiation, re-radiation, or reflection of electromagnetic energy with the objective of impairing the use of electronic devices, equipment, or systems. Interference is the radiation, emission, or indication of electromagnetic energy, unintentionally causing degradation, disruption, or complete obstruction of the designed function of the electronic equipment affected. Intent, not effect, is the deciding factor in determining if an event is classified intentional or unintentional.

Mean Power (of a radio transmitter)—The average power supplied to the antenna transmission line by a transmitter during an interval of time sufficiently long compared with the lowest frequency encountered in the modulation taken under normal operating conditions.

Mean-Time-Between-Failures (MTBF)—An indicator of expected system reliability calculated on a statistical basis from the known failure rates of various components of the system. The mean operating time between failures during which the item performs as specified. For a particular interval, the total functioning life of a population of an item divided by the total number of failures within the population during the measurement interval. The definition holds for time, cycles, miles, events, or other measure-of-life units.

Mean-Time-To-Repair (MTTR)—The total corrective maintenance time divided by the total number of corrective maintenance actions during a given period of time.

Media—In telecommunications, the paths along which the signal is propagated, such as wire pair, coaxial cable, waveguide, optical fiber, or radio path.

Medium Frequency (MF)—Frequencies of electromagnetic waves in the range from 300 kilohertz to 3 megahertz.

Mega (M)—A prefix denoting one million (10^6).

Megabyte (Mb)—In computing, a unit equal to 1,048,576 bytes.

Megacenter—A DISA/DISA WESTHEM-consolidated computer installation and its supporting organization providing computer processing, data storage, data communications, computer liaison support, and other related services. This includes building, operating, maintaining, and managing a computing and communications capability that supports command, control, business information systems/applications processing, and information transfer requirements; developing, deploying, operating, and maintaining information systems/applications; and providing training and information services. Also called Defense Megacenter (DMC).

Megahertz (MHz)—A unit of frequency denoting one million hertz.

Memory Scavenging—The collection of residual information from data storage.

Memory—In computing, any facility for holding data. It is often used to describe a computer's main or internal memory.

Menu—In computing, a list of options available within a software application.

Meridional Ray—In fiber optics, a ray of light that passes through the axis of the fiber as a result of internal reflection.

Mesochronous—The relationship between two signals such that their corresponding significant instants occur at the same average rate.

Message Indicator—Sequence of bits transmitted over a communications system for synchronizing cryptoequipment. Some off-line cryptosystems, such as the KL-51 and one-time pad systems, employ message indicators to establish decryption starting points.

Message Switching—A method of operating a communication network where messages are moved from node to node. The message switch at a node must be capable of storing a message, but need not necessarily wait for the whole message to be received before onward transmission.

Message—Any thought or idea expressed briefly in a plain or secret language and prepared in a form suitable for transmission by any means of communication.

Meta Principles—Principles that apply to the information technology environment as a whole. They address the organization's position on architecture, migration, and risk management, as well as its orientation to open or proprietary systems.

Metadata Database—A system that manages information about data as an enterprise.

Metadata—Information describing the characteristics of data; data or information about data; descriptive information about an organization's data, data activities, systems, and holdings.

Metallic Circuit—A circuit in which metallic conductors are used and in which the ground or earth forms no part.

Meteor Burst Communications—Communications by the propagation of radio signals reflected to earth by ionized meteor trails.

Meteorological Aids Service—A radio communications service used for meteorological and hydrological observation and exploitation.

Method of Collection—The mechanism, or method, by or through which an agency conducts or sponsors a collection of information from the public. This does not affect the requirement that the agency obtain and display a currently valid Office of Management and Budget control number on the collection, or the agency's obligation to disclose its estimate of the average burden hours per response. Collections of information may be conducted by mail or through personal or telephone interview, communications via electronic media, automated collection techniques, or any other approach through which the agency may question the respondent.

Metropolitan Area Network (MAN)—A system of links or a ring that interconnects a relatively high concentration of local area networks (LANs) together within a small regional area. It is normally used to connect numerous LANs together as well as to a wide area network (WAN). The MAN also provides routing and switching between the LANs as well as between the WLAN and the LANs. The demarcation points for the MAN are the service delivery nodes at the campus, base, post, or station router/switch and the hub/router/switch of the WAN.

Micro (mc)—A prefix used to denote one millionth (10^{-6}).

Microbend Loss—In fiber optics, the leakage of light caused by minute sharp curves in the optical cable

that may result from imperfections when the glass fiber meets the sheathing that covers it.

Microcircuit—Synonym for integrated circuit (IC).

Microcomputer—A computer in which the processing unit is a microprocessor and that usually consists of a microprocessor, a storage unit, an input channel, and an output channel, all of which may be on one chip.

MicroElectroMechanical System(s) (MEMS)—A relatively new technology which exploits the existing microelectronics infrastructure to create complex machines with micron feature sizes. These machines can have many functions, including sensing, communications, and actuation.

Microfiche—A sheet of film 105 by 148 millimeters (4 by 6 inches), containing multiple micro-images in a grid pattern. It usually contains a heading or title that can be read without magnification.

Microfilm—A fine grain, high resolution film containing an image or images greatly reduced in size from the original.

Microform—A generic form for any form, whether film, video tape, paper, or other medium, containing miniaturized or otherwise compressed images that cannot be read without special display devices.

Micrographics—The science and technology of recording information on, and retrieving it from, microform. It uses photographic techniques or computers to record images on film.

Micro—Prefix used to denote one millionth (10^6).

Microprocessor—A central processing unit implemented on a single chip.

Microprogram—A computer program written in the most basic or elemental instructions or subcommands a computer is capable of executing.

Microsecond—A unit of time equal to one millionth of a second.

Microwave—A term loosely applied to those frequency wavelengths that are sufficiently short to exhibit some of the properties of light waves (i.e., they are easily concentrated into a beam). Commonly used for frequencies from about 1-30 GHz.

Microwave Landing System (MLS)—A radio navigation system that provides the same information as an Instrument Landing System but operates in the 5000-5250 MHz band.

Microwave Radio Relay Station—A facility, part of a microwave radio telecommunications system, used for the reception and retransmission of microwave radio signals.

Middleware—A layer of hardware/software/communications introduced to interface a variety of workstation products with several incompatible database servers. The middleware integrates the data environment in a fashion that provides the user with the illusion of one federated database, despite the incompatibilities between the individual products. Although it is a commercial-of-the-shelf product, middleware systems are typically significant procurement items. It provides an expensive, but possibly cost-effective solution to tying the old with the new in a fashion compliant with the direction of interoperability in the DoD.

Migration System—An existing automated information system (AIS), or a planned and approved AIS, that has been officially designated to support common processes for a functional activity applicable to use DoD-wide or DoD component-wide. Systems in this category, even though fully deployed and operational, have been determined for transitioning to a new environment or infrastructure. A migration

system may need to undergo transition to the standard technical environment and standard definitions being established through the Defense Information Management Program, and must migrate toward that standard. In that process it must become compliant with the Reference Model and the Standards Profile. A system in this category may require detailed analysis that involves the total redesign, reprogramming, testing, and implementation because of a new environment and how the users have changed their work methods and processes. The detailed analysis may identify the difference between as is and the to be system.

Military/International Dispatch and Accountng System (MIDAS)—An interconnected US Postal Service automated processing and billing system for military and international mail.

Military Origin/Destination Information System—A US Postal Service system that uses manual and optical character reader technology to collect mail volumes, service analysis, and other mail characteristics data to measure the performance of systems that handle military mail.

Military Standard—A document that establishes uniform engineering and technical requirements for military-unique or substantially modified commercial processes, procedures, practices, and methods.

Milli (m)—Prefix used to denote one thousandth (10^{-3}).

Millisecond (msec)—One thousandth of a second.

Miniature Receive Terminal (MRT)—A radio receiver using the VLF/LF frequency spectrum. Primarily used for dissemination of Emergency Action Messages to the SIOP tasked forces.

Minimal Discernible Signal (MDS)—In radar, the minimum amount of target signal that san be seen above the noise level. MDS is a measurement (in decibels) of a signal-to-noise differential.

Minimal Protection (Class D)—Class reserved for those systems that have been evaluated but fail to meet the requirements for a higher evaluation.

Mission Bit Stream (MBS)—The total of subscriber information bits being passed through a system. This excludes framing, stuffing, control, and service channel bits.

Mission Need Statement (MNS)—A document, prepared by the respective using command or HQ USAF, that identifies an operational deficiency that cannot be satisfied through changes in tactics, strategies, doctrine, or training. A correction of the deficiency normally entails research and development, production, and procurement of a new system or modification of an existing system.

Mixed Excitation Linear Prediction (MELP)—A high performance speech coding algorithm for seamlesss interoperability across and between the strategic and/or tactical satellite communications and internetworking communications domains.

Mnemonic Symbol—A symbol intended to aid the human memory.

Mnemonic—Word or code symbolic of another word, code, or function.

Mobile Service—A service of radio communication between mobile and land stations, or between mobile stations.

Mobile Telephone Switching Office (MTSO)—Acts as the brains of the entire cellular system. It also serves to tie the cellular system to the Public Switched Telephone Network. The MTSO keeps constant track of the affiliation of all active cellular telephones on its system.

Modeling Service Standards—Modeling service standards simulate a condition or activity in a

transaction process system by performing a set of equations on a set of data. A model is a mathematical representation of a device or process used for analysis and planning.

Modeling—The application of a standard, rigorous, structured methodology to create and validate a physical, mathematical, or otherwise logical representation of a (C4) system, entity, phenomenon, or process.

Modem—Contraction of Modulator-Demodulator. In communications-electronics, a device that modulates and demodulates electrical (i.e., intelligence) signals.

Modification—Relative to configuration control, a configuration change to an already-produced configuration item, such as a communications system.

Modular C4 Packages—A set of capabilities and specific items of equipment matched to meet specific operational needs. Modular C4 packages can be interconnected to build C4 systems and networks to meet the needs of the mission.

Modulation Transfer Function (MTF)—A parameter using spatial frequency responses to characterize a screen display. The spatial frequency is stated in lines (line pairs) or minimum/maximum intensity pairs per unit distance. The MTF is used as a performance measurement of many optical systems.

Modulation—In communications-electronics, the encoding of information onto a carrier through the controlled variation of some characteristic of the carrier signal (for example, frequency, amplitude, and phase or combinations thereof). The modulated carrier wave serves to transport the signals within the system or between systems. The modulation process is normally associated with transmitting equipment. Transmission can be by cable/wire or by radio. In the system's associated receiving equipment, demodulation reverses the process and retrieves the original signals or information.

Modulator—An electronic device that imposes an intelligence signal on a carrier frequency. In radio communications, the modulator is part of the radio transmitter. Its size can vary from an entire rack of equipment to part of a circuit board, depending on the purpose, size, and radio frequency output power of the associated radio transmitter.

Module—In computing, a segment of core storage.

Monopulse—In radar, a method of determining azimuth and/or elevation angles simultaneously, as a result of only a one pulse transmission.

Motion Media—A series of images, taken with a motion picture or video camera, which, when viewed, gives the illusion of motion.

Moving Pictures Experts Group (MPEG)—A compression method of storing movie files in digital format.

Moving Target Indicator (MTI)—A radar receiver designed to reduce the effects of stationary clutter or slow moving weather.

Multi-Beam Antenna (MBA)—An antenna that provides multiple-shaped patterns for selected coverage areas on the earth's surface.

Multilevel Device—In information assurance, equipment trusted to properly maintain and separate data of different security categories.

Multilevel Mode—An information system's security mode of operation wherein all the following statements are satisfied concerning the users who have direct or indirect access to the system, its

peripherals, remote terminals, or remote hosts: (a) Some users do not have a valid security clearance for all the information processed in the Information System. (b) All users have the proper security clearance and appropriate formal access approval for that information to which they have access. (c) All users have a valid need-to-know only for information to which they have access.

Multi-Level Precedence and Preemption (MLPP)—The capability to originate calls based on precedence and to preempt calls of lower precedence already established within the network. Defense Switched Network precedence levels are: Priority, Immediate, Flash, and Flash Override.

Multilevel Security (MLS)—(1) Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization. (2) Concept of processing information with different classifications and categories that simultaneously permits access to users with different security clearances, but prevents users accessing information for which they lack authorization.

Multimedia—Pertaining to the processing and integrated presentation of information in more than one form. Multimedia deals with information consisting of still and motion imagery, audio, graphics, and text.

Multipath—In radio communications, the propagation phenomenon that results in a radio frequency signal reaching the receiving antenna by two or more separate paths. This may result in overall weakening or strengthening of the received signal, depending on the phase relationships of the signals.

Multiple Access—The capability of a communications satellite to function as a portion of a communications link between more than one pair of ground terminals simultaneously. Types of multiple access are: Frequency Division, Code Division, and Time Division.

Multiple Media—Transmission media using more than one type of transmission path (for example, fiber optics, radio, telephone line, and so forth) to deliver information.

Multiplex (MUX)—The process of combining multiple parallel information streams (voice and/or data channels) into a single communications channel. There are a number of different forms or methods of multiplexing. The most common (and oldest) forms are Frequency Division Multiplexing (FDM) and Time Division Multiplexing (TDM). In FDM each channel is assigned a separate frequency slot within the broader frequency channel of the communications path. In TDM, each channel is assigned a time slot within a time frame large enough to accommodate all channels.

Name Server—In computing, the name server provides a means of finding an attribute of an entity given the unique name for any entry within the technology environment. Entities can be physical components (computers, workstations, network nodes), logical components (application modules, data storage locations), or users. The name server will be accessed frequently by clients to find addresses for servers and other objects.

Nano (n)—A prefix used to denote one billionth (10^9)

Nanosecond(nsec)—One billionth of a second.

Narrowband Modem—A modem whose modulated output signal has an essential frequency spectrum that is limited to that which can be wholly contained within, and faithfully transmitted through, a voice channel with a nominal 4 kilohertz bandwidth.

Narrowband Signal—In telecommunications, any analog or analog representation of a digital signal whose essential spectral content is limited to that which can be contained within a voice channel of nominal 4 kilohertz bandwidth.

Narrowband—In data communications, pertaining to a channel with a bandwidth less than that of a voice-grade channel. It is normally used for communications speeds of less than 300 bits per second.

National Communications System (NCS)—The telecommunications system that has resulted from the technical and operational integration of the separate telecommunications systems of 22 Federal member departments and agencies, including the DoD, and is responsible to ensure the availability of a viable national security and emergency preparedness telecommunications infrastructure. The NCS consists of the telecommunications assets of the entities represented on the NCS Committee of Principals and an administrative structure consisting of the Executive Agent, the NCS Committee of Principals, and the Manager. The NCS Committee of Principals consists of representatives from those Federal departments, agencies, or entities designated by the President that lease or own telecommunications facilities or services of significance to national security or emergency preparedness. Although the DoD's Global Information Grid (GIG) is a large part of the NCS, the NCS is much broader in scope.

National Information Infrastructure (NII)—The nationwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The NII encompasses a wide range of communications and information equipment, systems, and networks, including the personnel who make decisions and handle the transmitted information. The NII is similar in nature and purpose to the Global Information Infrastructure but relates in scope only to a national information environment, which includes all government and civilian information infrastructures.

National Institute for Standards and Technology (NIST)—Formerly National Bureau of Standards. The division of the U.S. Department of Commerce that ensures standardization within government agencies. NIST is responsible for the Applications Portability Profile, a set of standards and guidelines for U.S. Government procurement.

National Security Information—Any information that has been determined pursuant to Executive Order 12356 or any predecessor order to require protection against unauthorized disclosure and is so designated.

National Security System—Any telecommunications or information system operated by the United States Government, the function, operation, or use which: (1) involves intelligence activities; (2) involves crytologic activities related to national security; (3) involves command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons system, or (5) is critical to the direct fulfillment of military or intelligence missions. (This does not include a system that is to be used for routine administrative and business applications, including payroll, finance, logistics, and personnel management applications). (DoD 8000.1)

National Security Telecommunications and Information Systems Security Instruction (NSTISSI)—

A series of documents that establishes the technical criteria for specific national security telecommunications and automated information systems security matters.

Neper (Np)—In telecommunications, a unit used to express signal gain or loss and relative power ratios. The neper is analogous to the decibel, except that the Naperian base 2.71828 is used in computing the ratio in nepers. One neper (Np) = 8.686 dB. The neper is often used to express voltage and current ratios, whereas the decibel is usually used to express power ratios. Like the dB, the Np is a dimensionless unit. Where the decibel is commonly used in the United States, the neper is commonly used in Europe.

Net Gain/Loss—The overall gain or loss of a transmission circuit.

Network Layer—In data communications, a layer in the International Standards Organization's open systems interconnection.

Network Management—The ability to provide fault management, configuration management, security management, accountancy management, and performance management for the network.

Network Mapping (NMAP)—NMAP is information on specific information systems consisting of type of hardware, software loaded in the information systems, operational description, criticality of information systems, accreditation status and date, sensitivity, location, IP address, and systems administrator points of contact.

Network Operations (Global Information Grid [GIG])—Organizations and procedures required to monitor, manage, and control the GIG. Network operations incorporates network management, information dissemination management, and information assurance.

Network Protocols—The standardized agreements and their hardware or software implementations used to control the orderly exchange of information on a network and associated data links.

Network Security—The protection of networks and their services from destruction, unauthorized modification, or disclosure providing an assurance that the network performs its critical functions correctly and that there are no harmful side-effects.

Network Sponsor—Individual or organization responsible for stating the security policy enforced by the network, for designing the network security architecture to properly enforce that policy, and for ensuring that the network is implemented in such a way that the policy is enforced. For commercial-off-the-shelf systems, the network sponsor will normally be the vendor. For a fielded network system, the sponsor will normally be the project manager or system administrator.

Network System—System implemented with a collection of interconnected components. A network system is based on a coherent security architecture and design.

Network Topology—The specific physical or logical arrangement of the elements of a network.

Network Trusted Computing Base (NTCB) Partition—Totality of mechanisms within a single network component for enforcing the network policy, as allocated to that component; the part of the NTCB within a single network component.

Network Trusted Computing Base (NTCB)—Totality of protection mechanisms within a network, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. See trusted computing base.

Network Warfare Simulation (NETWARS)—The standard DoD approved communications simulation tool. Commanders-in-Chief, the Services, and DoD agencies use NETWARS for communications modeling purposes.

Network Weaving—Penetration technique in which different communication networks are linked to access a communications and informaton system to avoid detection and trace-back.

Network—(1) An organization of stations capable of intercommunication but not necessarily on the same channel. (2) Two or more interrelated communications circuits. (3) A system of software and hardware connected to support the exchange of data. (4) A combination of circuits and terminals serviced by a single switching or processing center. (5) Two or more systems connected by a communications medium.

Networthiness-—A networthiness assessment determines impacts, risks, and vulnerabilities of fielding

a system. The assessment is based on a particular system configuration implemented in a target Air Force environment. Parameters that are assessed include: network security, network impact, compatibility with the infrastructure, infrastructure requirements, spectrum support, security policy compliance, JTA/ JTA-AF standards compliance, communications and information manpower, training, logistics support, schedule, and funding.

Networthy-—A networthy system or application has been assessed and determined to be supportable from a communications and information perspective, and any impacts, risks, and vulnerabilities it may present to the enterprise are deemed to be acceptable or manageable.

Nodal Switch—A tandem switch in the DSN that connects multiple end offices, provide access to a variety of transmission media, route calls to other nodal switches, and provide network features such as multilevel precedence and preemption. There are two types of nodal switches in the DSN, stand-alone and multifunction switches.

Node—(1) A location in a mobility system where a movement requirement is originated, processed for onward movement, or terminated. In network topology, a terminal of any branch of a network or a terminal. (2) A point in a network, either at the end of a communications line (end node) or where two lines meet (intermediate node). (3) In switched communications, a node is the switching point that may also include patching and control facilities. (4) In a data network it is the location of a data station that interconnects data transmission lines. (5) A point in a standing or stationary electromagnetic wave at which the amplitude is minimum.

Noise Level—In telecommunications, the volume of noise power on a circuit or channel, measured in decibels, usually referenced to a base (such as milliwatt, dBm)

Noise Suppression—(1) The reduction of the noise power level in electrical circuits. (2) In radio communications, the process of automatically reducing the (audible) noise in the output of a radio receiver during periods when a carrier is not being received. (Compare: squelch.)

Noise—In telecommunications, (1) An undesired disturbance within the useful frequency band; the summation of unwanted or disturbing energy introduced into a communications system from man-made and natural sources. (2) A disturbance that affects a signal and that may distort the information carried by the signal. There are many and varied types of noise in a telecommunications system.

Nomenclature—In the Joint Electronics Type Designator System (JTEDS), the combination of an item name and type designation, such as of communications equipment/system, e.g., VHF/UHF Radio Set, AN/TRC-24.

Nominal Bandwidth—The widest band of frequencies, inclusive of guard bands, assigned to a communications channel.

Noncritical Technical Load—That part of the technical (electrical) load of a communications facility not for equipment requiring synchronous operation.

Non-Developmental Item (NDI)—(1) Any hardware or software item commercially available in the market place. (2) Any commercial-off-the-shelf (COTS) item.

Non-directive Publication—A publication that is informational and suggests guidance that can be modified to fit the circumstances. Compliance with publications in this category is expected, but not required.

Non-Discretionary Security—Aspect of DoD security policy that restricts access on the basis of security

levels. A security level is composed of a read level and a category set restriction. For read-access to an item of information, a user must have a clearance level greater than or equal to the classification of the information, and have a category clearance that includes all the access categories specified for the information.

Non-Form Item—A printed product without spaces for entering information. Some non-form items have been entered into the Standard and Optional Form Program so they can be controlled government-wide.

Non-Kernel Security-Related Software (NKSR)—Security-relevant software that is executed in the environment provided by a security kernel rather than as a part of the kernel itself.

Non-processed Satellite Channel—In satellite communications, a channel that uses a non-regenerative transponder.

Nonrecord—Information materials that are not part of the legal definition of a record. Includes extra copies of documents kept only for convenience of reference, stocks of publications and of processed documents, and library or museum materials intended solely for reference or exhibition.

Nonrecurring Pamphlets—Nondirective classified or unclassified publications printed once. They are usually published to inform, motivate, increase knowledge, or improve performance. The term includes leaflets, bulletins, folders, booklets, reports, and similar nonrecurring pamphlets.

Non-regenerative Transponder—In satellite communications, a transponder that is capable only of receiving, amplifying, frequency translating, and retransmitting a received signal.

Nonrepudiation—Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can deny having processed the data.

Non-Return-To-Zero (NRZ) Code—A code having two states termed zero and one, and no neutral or rest condition.

Non-Secret Encryption (CFD)—Synonymous with Public Key Cryptography.

Non-Secure (SBU) Internet Protocol (IP) Router Network—A high-speed unclassified data network for DoD that provides interconnectivity among DoD customers and the commercial network.

Nontechnical Load—In a communications installation, that part of the total operational (electrical) load used for general lighting, ventilation, air conditioning, and so forth, required for normal operation.

N-Type Material—In electronics, a semi-conductor material doped with an impurity that provides nuclei with loosely bound electrons. These electrons provide negative charge carriers and are the source of current flow through the semi-conductor device.

Nuclear Hardness—(1) The measure or extent to which performance of a communications system will degrade in a given nuclear environment. (2) The physical attributes of a system or component that will allow a defined degree of survivability in an environment that includes nuclear radiation and electromagnetic impulse.

Null Character—In data communications, a control character that is used as a fill character for transmission or storage. It may be removed from a sequence of characters without affecting its meaning. The null character may, however, have some significance in the control of equipment or formatting.

Null String—In data structures, a string that contains no characters.

Null—(1) In cryptography, a dummy letter, letter symbol, or code group inserted in an encrypted message

to delay or prevent its decryption or to complete encrypted groups for transmission or transmission security purposes. (2) In an antenna radiation pattern, a zone in which the effective radiated power is at a minimum relative to the maximum effective radiated power of the main beam. (3) In radar, a point of minimum or no detection.

Nyquist Sampling Theorem—In digital communications, a theorem that specifies the sampling rate necessary to ensure the original analog signal can be reconstituted from the sampled values. The theorem states the sampling rate must be twice as high as the highest frequency present in the sampled signal.

Object Based Language—A programming language that supports some but not all of the characteristics of abstraction, encapsulation, modularity, and hierarchy.

Object Code—The final result of a language translation; a set of bit patterns interpretable by the electronic circuitry of a computer.

Object Database—A database that holds abstract data types (objects). It can store objects directly from an object-oriented programming language.

Object Link Embedding (OLE)—In computing, a method to transfer and share information between applications. OLE links are similar to direct data exchange (DDE) links, except the source (server) application can be started from within the current (client or receiving) application to edit the linked object. An OLE object can be linked or embedded. A linked OLE object leaves the data stored in the source (server) application file. In an embedded OLE object, the data for the object is stored in the current (client or receiving) application file.

Object Oriented Language—A programming language that fully supports the characteristics of abstraction, encapsulation, modularity, and hierarchy.

Object—A passive receiver of information. Access to an object implies access to the information the object contains. Examples of objects are: records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, and network nodes. A person, place, thing, concept, event, or activity about which an organization keeps information.

Objective Configuration—A configuration that depicts the organization optimum information and resource capabilities needed to support the mission.

Obsolete Publication—A rescinded or superseded publication.

Offensive Counterinformation (OCI)—Offensive information warfare activities which are conducted to control the information environment by denying, degrading, disrupting, destroying, and deceiving the adversary's information and information systems.

Offensive Information Operations (OIO)—A subset of Information Operations (IO). The integrated use of assigned and supporting capabilities and processes, mutually supported by intelligence, to affect information and information systems to achieve or promote specific objectives. These capabilities and processes include, but are not limited to, operations security, military deception, psychological operations, electronic warfare, and physical destruction.

Off-Hook—In communications, a condition in which a unit indicates a busy condition to incoming telephone calls.

Off-The-Shelf (OTS)—Procurement of existing systems or equipment without a research, development,

test, and evaluation (RDT&E) program or with minor development to make the item suitable for Department of Defense needs.

Office Automation—In office systems, the use of any form of machine or system that either replaces or simplifies human activities and operations in office environments.

Office Forms—Forms for use only within the originating directorate, division, branch, or section. Major command and field operating agency Information Managers may delegate the control of office forms to the office of primary responsibility. Office forms do not have to be prescribed, and indexing them is optional.

Office of Primary Responsibility (OPR)—Any organizational activity having primary functional interest in, and responsibility for a specific action, project, plan, or program.

Official Mail—Any item processed through the United States Postal Service that pertains exclusively to the business of the United States Government for which the postage and fees are paid by the United States Government.

Official Record—Recorded information, regardless of media, maintained by an agency to comply with its legal obligations or created as a result of its transactions of public business. Excluded as records are library and museum materials, extra copies of documents preserved for convenience or references, stocks of publications, and blank forms.

Off-Line—That condition where devices or subsystems are not connected into, do not form a part of, and are not subject to the same controls as an operational system. These devices may, however, be operated independently.

Omni-Directional Antenna—An antenna whose radiation pattern is non-directional in azimuth.

On Call—In satellite communications, a link which does not continuously transfer information; the telecommunications sessions supporting information transfer are activated and released on-demand as needed.

One-Time Cryptosystem—A cryptosystem employing key used only once.

One-Time Form—A forms that satisfies a one-time requirement, is not reprinted, and is obsolete when no longer needed.

One-Time Request—The customer may obtain an order quantity on a one-time basis without changing their average monthly usage.

On-Hook—In telephony, a condition in which the telephone is not in use.

On-Line Processing—Processing where individual transactions are entered into the equipment via a terminal. The data entry is processed and a response is transmitted back to the terminal for user dissemination.

Ontology—A structured, language dependent network of linked concepts that describes the world or a subset of the world. The study of being or existence.

Open Circuit—1. In communications-electronics, a circuit that contains an infinite (very high) impedance, for example, a circuit that is not connected or not terminated properly. 2. A communications circuit that is available for use. An open circuit may be intentional, as in a switch, or may constitute a fault, as in a severed cable.

Open Loop—A system in which the input signal or information is not influenced by the output of the system.

Open Network—A network that can communicate with any system component (peripherals, computers, or other networks) implemented to the international standard (without special protocol conversion, such as gateways). Also see Open System.

Open Security Environment (CFD)—Environment that does not provide sufficient assurance that applications and equipment are protected against the loss of confidentiality, integrity, or availability.

Open Software Foundation (OSF)—A consortium of computer hardware and software manufacturers whose membership includes many of the computer industry's leading companies.

Open Source Software—Free software that is available in source code form. It does not have any licensing restrictions to limit its use, modification, or distribution.

Open Specification—Public specifications that are maintained by an open, public consensus process to accommodate new technologies over time and that are consistent with international standards.

Open Standards—Widely accepted and supported standards set by recognized standards organizations or the market place. Open standards support interoperability, portability, and scalability and are equally available to the general public.

Open Storage—Storage of classified information within an accredited facility, but not in General Services Administration-approved secure containers, while the facility is unoccupied by authorized personnel.

Open System—(1) A (communications) system with specified standards that can be readily connected to other systems that comply with the same standards. (2) A system that implements sufficient open specifications for interfaces, services, and supporting formats to enable properly engineered components (a) to be utilized across a wide range of systems with minimal change, (b) to interoperate with other components on local and remote systems, and (c) to interact with users in a manner that facilitates user portability. (3) A communications and information system that is accessed or observed by users outside the system and that provides information by open sources or operational security (OPSEC) indicators. Open information systems use open source information to provide OPSEC indicators that my be observed by adversaries. Open systems may also be influenced, jammed, interrupted, or exploited by adversaries and adversarial weapons systems. Examples of open systems are: nonsecured telephone systems, computer systems connected to outside lines, and unsecured radio systems.

Open Systems Application Program Interface (API)—A combination of standards-based interfaces specifying a complete interface between an application program and the underlying application platform.

Open Systems Architecture—The framework describing the entities (for example, components and services) and their interrelationships in an open system. Open system architectures and environments are intended to help achieve portability, interoperability, scalability, and cost-effectiveness of systems.

Open Systems Environment (OSE)—A comprehensive set of interfaces, services, and supporting formats, plus aspects for interoperability of application, as specified by information technology standards and profiles. An OSE enables information systems to be developed, operated, and maintained independent of application specific technical solutions or vendor products.

Open Systems Interconnection (OSI)—Concept for achieving total interoperability of information systems based on a layered, structured hierarchy of specific technical functions required for information

transfer. Implies vendor independence in most circumstances.

Open Systems Interconnection Reference Model (ISO-RM)—In data communications, an ISO-RM is intended to coordinate the development of communications interfaces and protocol standards at all levels of communications. The OSI model defines seven functional layers with standardized interfaces between them. The concept of the layers provides for a considerable degree of independence between the multifarious and complicated operations involved in data communications. At each level the process believes it is communicating with its corresponding layer in the receiving host.

Open Wire—In telecommunications, unshielded wire conductors separately supported above the surface of the earth.

Operating Document—A completed form or other document used to facilitate, accomplish, or provide a description or record of a transaction, function, or event. The information in an operating document may provide data or input for a report, but that is not its primary purpose. Examples of operating documents include application forms, purchase orders, personnel actions, bills of lading, payrolls and time sheets, inspection or audit reports, and reports that involve direct command and control of military forces or cryptological activities related to national security.

Operating System—(1) The system that controls a computer's activities, and by which it uses applications programs. (2) An integrated collection of service routines for supervising the sequencing and processing of programs by a computer. Operating systems control the allocation of resources to users and their programs and play a central role in operating a computer system. Operating systems may perform input or output, accounting, resource allocation, storage assignment tasks, and other system-related functions.

Operational Architecture—A description (often graphical) of the operational elements, assigned tasks and information flows required to accomplish or support a DoD function or military operation. It contains descriptions of the operational elements, assigned tasks and activities, and information flows required to support the warfighter. It defines the types of information exchanged, the frequency of exchange, which tasks and activities are supported by the information exchanges, and the nature of information exchanges in sufficient detail to ascertain specific interoperability requirements. Also referred to as "functional architecture."

Operational Area Network (OAN)—Networks created out of assets organic to deployed units, or serving principally to connect deployed units to each other. This is normally the primary mechanism for establishing the Theater Joint Tactical Network (TJTN) from individual Service-deployed Campus Area Networks (CAN) and Local Area Networks (LAN) supporting their tactical forces, and interfacing with the Defense Information System Network (DISN) Wide Area Network (WAN).

Operational Data Security—Protection of data from either accidental or unauthorized intentional modification, destruction, or disclosure during input, processing, storage, transmission, or output operations.

Operational Key—Key intended for use on-the-air for protection of operational information or for the production or secure electrical transmission of key streams.

Operational Load—The total electrical power requirements for a communications facility.

Operational Requirements Document (ORD)—A formatted statement containing performance and related operational parameters for the proposed concept or system. It is prepared by the user or user's representative at each acquisition program milestone beginning with milestone I.

Operational Test and Evaluation (OT&E)—Testing and evaluation conducted in as realistic conditions as possible throughout the system's life cycle. Tests are conducted to verify that an information system is installed and capable of performing its operational mission as outlined in program documentation. OT&E is used to verify operating instructions, computer documentation, training programs, publications, and handbooks.

Operational Waiver—Authority for continued use of unmodified communications security end items, pending the completion of a mandatory modification.

Operations Security(OPSEC)—A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities (1) to identify those actions that can be observed by adversary intelligence systems, (2) determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and (3) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

Optical Character Recognition (OCR)—(1) The analysis and translation of a graphic representation of text into a coded form such as American Standard Code for Information Interchange (ASCII) or Extended Binary Coded Decimal Interchange Code (EBCDIC). (2) The method of inputting data into a computer by reading printed or hand-written characters.

Optical Crosstalk—Optical crosstalk, or bleeding, occurs when the light from the incorrect video image gets through. When referring to stereoscopic images, the right eye's image is visible to the left eye or vice versa.

Optical Digital Technologies (ODT)—Represent technologies that use the reflective properties of light and an optical recording surface to capture, encode, decode, and store data. ODT predominantly encompass optical media, optical drives, and scanners.

Optical Instrumentation—Use of optical systems, coupled with photographic or television recording devices, that may include audio, to record scientific and engineering phenomena for the purpose of technical measurement and evaluation. It may also include recording data to correlate optical images to time or space positions or other engineering data.

Optional Modification—A National Security Agency-approved modification not required for universal implementation by all holders of a communications security end item. This class of modification requires all of the engineering/doctrinal control of mandatory modification, but is usually not related to security, safety, TEMPEST, or reliability.

Orange Book—The DoD Trusted Computer System Evaluation Criteria (DoD 5200.28-STD).

Order Source—In this functional description, an order source is the office the user has an account with.

Orderwire Circuit—In telecommunications, a voice or data circuit used by technical control and maintenance personnel to coordinate operations and maintenance actions for the control and restoration of communications circuits and systems.

Oscillator—In electronics, a circuit or device that produces a sinusoidal, square wave, or pulsed signal of a specified frequency. These signals are used in radio and communications equipment for a variety of purposes, such as tone or frequency generators, and for timing and synchronization.

Out-Of-Band Signaling—Signaling that utilizes frequencies within the guard band between channels or bits other than information bits in a digital system.

Out-Of-Phase—In electronics, referring to signals that exhibit a shift in the phase (of a voltage or current) relative to each other. When such out-of-phase signals are combined, the difference in their phases generally causes a cancelling effect, resulting in a weaker signal or a completely cancelled-out signal, depending on the degree of the phase differences.

Outside Plant—That portion of intrabase communications systems extending from the main distribution frame outward to the telephone instrument or the terminal connections for other technical components.

Ovality—In an optical fiber, the degree of deviation from perfect circularity of the cross-section of the core or cladding.

Overhead Bit—A bit other than an information bit. Included for control or error-checking purposes.

Overmodulation—The condition that prevails when the instantaneous level of the modulating signal exceeds the value necessary to produce 100 percent modulation of the carrier.

Overprinting—The printing of pertinent repetitive information (e.g., agency name, accounting codes, etc.) in a caption area on a form.

Over-The-Air Key Distribution—Providing electronic key via over-the-air rekeying, over-the-air key transfer, or cooperative key generation.

Over-The-Air Key Transfer—Electronically distributing key without changing traffic encryption key used on the secured communications path over which the transfer is accomplished.

Over-The-Air Rekeying (OTAR)—Changing traffic encryption key or transmission security key in remote cryptoequipment by sending new key directly to the remote cryptoequipment over the communications path it secures.

Overtones—In communications-electronics, frequencies that are multiples of the fundamental frequency.

Overwrite Procedure—Process of writing patterns of data on top of the data stored on a magnetic medium.

Packet Internet Groper (PING)—In Transmission Control Protocol/Internet Protocol, a protocol function that tests the ability of a computer to communicate with a remote computer by sending a query and receiving a confirmation response.

Packet Switching—A data transmission process, utilizing addressed packets, where a channel is occupied only for the duration of transmission of the packet. A method of message transmission in which each completed message is assembled into one or more packets that can be sent through the network, collected and re-assembled into the original message at the destination. The individual packets need not be sent by the same route.

Packet—A group of binary digits including data and control elements that is switched and transmitted as a composite whole. The data and control elements, and possibly error control information, are arranged in a specified format.

Pager—A small radio receiver designed to be carried conveniently on one's person and give an aural, visual or tactile indication, when activated by reception of a radio signal containing its specific code. A pager is usually capable of displaying messages (alphanumeric characters), and may also be able to reproduce sounds. Some pagers also transmit a radio signal back to the message center, to acknowledge receipt of the paging message. Also called a beeper.

Paired Cable—A cable made up of one or more separately insulated pairs or lines, none of which are

arranged with others to form quads. See also Quadded Cable.

Palm-top—A small (pocket-size), hand-held computer, often including network-access software, personal-schedule software, and a basic word processor.

Parabolic Antenna—An antenna consisting of a parabolic reflector and a radiating or receiving element at or near its focus.

Parallel Port—A port through which two or more data bits are passed simultaneously, such as all the bits of an 8-bit byte, and that requires as many input channels as the number of bits that are to be handled simultaneously.

Parallel Transmission—In data communications, the simultaneous transmission of signal elements constituting the same code (for example, each bit of a word is sent simultaneously on an individual wire). It has a higher bit rate then corresponding serial transmission, but requires eight wires to convey individual bytes and is therefore mainly used for transmission over short distances.

Parameter—Quantity or constant whose value varies with the circumstances of the application.

Parametric Amplifier—A radio frequency amplifier that has a very low noise level and is especially designed to amplify very weak signals. In radio communications, the parametric amplifier is used in the receivers of satellite earth terminals and wideband radio communications systems.

Parity—In binary-coded systems, a condition obtained with a self-checking code such that in any permissible code expression the total number of ones or zeroes is always even or odd.

Parity Bit—In data communications, an extra bit that can be added to a group of “0” bits and “1” bits to make the parity of the group odd or even. The parity bit is discarded when the message is received.

Parity Check—A check that tests whether the number of ones (or zeroes) in an array of binary digits is odd or even. Odd parity is standard for synchronous transmission and even parity for asynchronous transmission.

Partitioned Security Mode—Information system security mode of operation wherein all personnel have the clearance, but not necessarily formal access approval and need to know, for all information handled by an information system.

Passband—In communications, the range of signal frequencies that can be satisfactorily transmitted on a given channel (for example, the passband on voice-grade channels is 300-3400 hertz).

Passive Device—A device that does not require a source of energy for its operation. Examples of passive devices are resistors, capacitors, diodes, filters, and so forth.

Passive Repeater—In microwave radio communications, an unpowered device used to route a microwave radio beam over or around an obstruction, such as a hill or mountain ridge, where the installation of a powered repeater is not feasible. Examples of a passive repeater are two parabolic antennas connected back-to-back, and a flat, billboard type reflector used as a mirror to deflect the radio beam.

Passphrase—Sequence of characters, longer than the acceptable length of a password, that is transformed by a password system into a virtual password of acceptable length.

Password—(1) A secret word or distinctive sound used to reply to a challenge. (2) A protected word or string of characters that identifies or authenticates a user for access to a specific system, data set, file, record, etc.

Patch—(1) In telecommunications, to connect circuits together, usually temporarily, by means of a cord (cable) known as a patch cord. (2) In computer programming, (a) to replace a small set of instructions with a modified or corrected set; and (b) to modify a program by changing its object code rather than its source code

Patch and Test Facility—An organic element of a communications station or terminal facility that functions as a supporting activity, under the technical supervision of a designated technical control facility.

Patch Bay—In telecommunications, an assembly of hardware so arranged that a number of circuits, usually of the same or similar type, appear on jacks for monitoring, interconnecting, and testing purposes. Patch bays are used in technical control facilities, patch and test facilities, and telephone exchanges.

Patch Panel—A segment of a Patch Bay.

Path Diversity—In satellite communications, the ability to simultaneously communicate with multiple satellites.

Path Loss—The decrease in power in transmission from one point to another along a propagation path. In radio communications systems, it is taken as the loss in power of the radio signal between the transmitter and receiver antennas, expressed in decibels.

Path Profile—A graphic representation of the physical features of a propagation path in the vertical plane, containing both end points of the path, showing the surface of the earth as well as buildings, trees, and other obstacles that may obstruct the radio signal.

Peak Envelope Power (PEP) (of a radio transmitter)—The average power supplied to the antenna transmission line by a transmitter during one radio frequency cycle at the crest of the modulation envelope taken under normal operating conditions.

Penetration—(1) Unauthorized act of by-passing the security mechanisms of a system. (2) The successful unauthorized access to an AIS or act of by-passing the AIS security controls.

Performance Standard—General design criteria that define the desired result without specifying the techniques for achieving that result.

Perigee—In satellite communications, the point at which a satellite is at a minimum distance from the earth in its orbit. Compare Apogee.

Periodic Antenna—An antenna that has an approximately constant input impedance over a narrow range of frequencies. Synonym: Resonant Antenna.

Periodical—Any classified or unclassified Air Force magazine or newsletter publication (with a consistent format, content, and purpose) published at least once a year to provide information pertinent to the publishing activity. Its purpose is to disseminate information and material necessary to the issuing activity. Periodicals may refer to or quote directive information, but are not directive publications.

Periods Processing—(1) Processing of various levels of classified and unclassified information at distinctly different times. Under the concept of periods processing, the system must be purged of all information from one processing period before transitioning to the next. (2) Processing of various levels of classified and unclassified information at distinctly different times. ***NOTE:*** Under periods processing, the AIS (operating in dedicated security mode) is purged of all information from one processing period before the next when there are different users with different authorizations.

Peripheral—In computing, a device, under control of the central processing unit, that performs an auxiliary action in the system (for example, input/output, backing, storage).

Peripheral Equipment—(1) n data processing, any equipment distinct from the central processing unit that may provide the system with additional capabilities. (2) Any equipment that provides the computer with additional capabilities distinct from the central processing unit; for example, a printer, scanner, mouse, keyboard, etc.

Peripheral Interface Adapter (PIA)—In computing, a device that provides interface functions between the computer bus and its peripherals.

Permanent Records—Records the Archivist of the United States has appraised and approved for permanent retention by the United States Government, and for accessioning into the National Archives.

Permuter—Device used in cryptoequipment to change the order in which the contents of a shift register are used in various nonlinear combining circuits.

Personal Computer Memory Card International Association (PCMCIA)—The organization of marketing and engineering professionals that defines the standard for the form and interconnection method of credit card size enclosed circuit boards that add various peripherals and memory storage, particularly for laptop computers and personal digital assistants. Also refers to the technology.

Personal Digital Assistant (PDA)—A hand-held computer, usually with a pen-based user interface and wireless communications capability for fax, data, and paging.

Personal Identifier—A name, number or symbol that is unique to an individual, usually the person's name or Social Security number.

Peta (P)—A prefix denoting 1000 trillion (10^{15}). (This quantity is increasingly used within the imagery community).

Phase Hit—In a telecommunications channel or circuit, a momentary disturbance caused by sudden phase changes in the signal.

Phase Jitter—In communications-electronics, rapid, repeated phase disturbances in a data or analog signal that result in the intermittent shortening or lengthening of signal elements.

Phase Locked Loop (PLL)—In communications-electronics, an electronic circuit that serves as a frequency control or stabilizing device; it controls a frequency generator (oscillator) so that it maintains a constant phase angle relative to a reference signal.

Phase Modulation—In radio communications, a method of modulation in which the phase of the sinusoidal carrier is varied in accordance with the modulating signal. Compare frequency modulation.

Phase Shift—In electronics, the change in phase of a periodic signal in relation to a reference of the same or another signal.

Phase Shift Keying (PSK)—In data communications, a method of changing the phase of the sinusoidal signal to represent binary data. If only two discrete phases are employed, each phase corresponds to a binary 1 or 0; if four phase shifts are used each one may correspond to a dibit.

Phased Array—An arrangement of antennas (of any type) in which the signal feeding each antenna is varied in such a way that radiation is reinforced in a desired direction and suppressed in undesired directions. Rapid scanning in azimuth or elevation can be accomplished with such arrays.

Pica—A printer's unit of measure used principally in typesetting. One pica equals approximately one-sixth of an inch. A pica gauge is the printer's measuring tool. There are 12 points to 1 pica, or 6 picas to 1 inch. The length of the line is specified in picas, as well as the depth of a type area. Inches are not used in type measurement.

Pico (p)—A prefix used to denote one trillionth (10^{12}).

Picowatt(pW)—A unit of electrical power equal to one trillionth of a watt.

Piece Part—In communications-electronics maintenance, a single piece not normally subject to disassembly without destruction or impairment of its use, such as resistors, capacitors, transistors, relays, gears, etc.

Piezoelectric—Relating to the generation of electricity or an electric polarity due to pressure exerted in or on a crystalline structure.

Pilot (frequency)—In telecommunications, a signal, usually a single frequency, transmitted over a system for supervisory, control, synchronization, or reference purposes.

Pitch—The number of characters in 1 inch along a typed line. This measure does not apply to proportional spacing. Also, pitch is sometimes used as another term for character spacing.

Pixel—Contraction for picture element. A pixel is a single dot on a (computer monitor) display screen.

Plain Text—In information assurance, unencrypted information.

Planar Array—An antenna in which all of the elements, both active and passive, are in one plane.

Plant—All the facilities and equipment used to provide telecommunications services.

Plesiochronous—In time division multiplexing, the relationship between two signals such that their corresponding significant instants occur at nominally the same rate, any variations being constrained within a specific limit.

Plug-In—In computing, a small software program that adds functionality to a browser (or other software program), that is not included in the basic program. Plug-ins can add the capability to hear music or other sounds and watch full-motion video or other multimedia presentations.

Point of Presence (POP)—In computer networking, a geographical location, typically a town or city, where a network can be connected to, often with dial-up telephone lines.

Polar Orbit—An earth orbit in which the angle of inclination is 90 degrees. A satellite in polar orbit will pass over both the north and south geographic poles once per orbit.

Polarization—That property of a radiated electromagnetic wave describing the time varying direction and amplitude of the electric field vector. The position of an antenna is described according to the polarization of the electric field of the radio wave emitted from, or received by, the active element of the antenna. For example, in a horizontally polarized antenna, the active element is horizontal to the surface of the earth.

Antennas are horizontally, vertically, or left or right circularly polarized.

Policy—A statement of important, corporate level direction that guides Air Force decisions. Policy is enforceable, and compliance with policy is measurable. Policy is the framework connecting the abstract ideas or principles contained in vision, mission, and purpose statements to the specific and concrete

statements of plans, goals, and objectives. Policy can be viewed as establishing bounds within which the organization will operate. Policy provides both a focus for Air Force action and a guide for the behavior of the organization and its members.

Portability—The ease with which software can be transferred from one information system to another.

Portable Operating System Interface for Computer Environments (POSIX)—(1) The term POSIX has been evolving into a term with a number of different meanings. POSIX is sometimes used to denote the formal standard ISO/IEC 9945-1, sometimes to denote that standard plus related standards and drafts emerging from IEEE P1003.x working groups, and sometimes to denote the groups themselves. Reference is preferred to the original POSIX standard by its standard designation ISO/IEC 9945-1 and not by the term POSIX. (2) A collection of evolving standards intended to provide a common interface and functionality for applications to access operating system services.

Portal—A term used to describe a Web site that is or is intended to be the first place seen when using the Web. Typically, a portal site has a catalog of websites, a search engine, or both. A portal site may also offer e-mail and other services to entice web users to use that site as their main point of entry to the Web, hence the term portal. A term used to describe a Web site that is or is intended to be the first place seen when using the Web. Typically, a portal site has a catalog of websites, a search engine, or both. A portal site may also offer e-mail and other services to entice web users to use that site as their main point of entry to the Web, hence the term portal.

Positive Control Material—Generic term referring to a sealed authenticator system, permissive action link, coded switch system, positive enable system, or nuclear command and control documents, material, or devices.

Positive Feedback—In electronics, a signal feedback arrangement in which part or all of the output signal of a device, usually an amplifier, is effectively added to the input signal or fed back into the input circuit for gain control or circuit stabilization purposes. Under certain conditions this can result in self-sustained oscillations.

Post Office Protocol (POP)—A protocol designed to allow single users to read mail from a server. There are three versions: POP, POP2, and POP3. The POP is used to transmit the stored mail from the server to the user's local mailbox on the user's client machine.

Postalize—In telecommunications, to structure rates or prices so that they are not distance sensitive, but depend on other factors, such as call duration, time of service, and time of day.

Posting—Adding or removing pages, or writing in changes or items from a supplement to a basic publication.

Power Absorbing Device (PAD)—In telecommunications, a device or circuit of electronic components designed to attenuate audio or radio frequency signals by a pre-determined amount with a minimum of distortion to the signals.

Precedence—In telecommunications, a ranking assigned to indicate the degree of preference to be given in the processing and protecting of a telephone call. Originators of a precedence call may elect to use their highest authorized precedence or any lesser precedence. Precedence levels (from lowest to highest) are: Routine, Priority, Immediate, Flash, and Flash Override.

Predictive Modeling—Use of a model to predict the actual response of a system or process.

Preferred Products List (PPL)—List of commercially produced equipment that meet TEMPEST and

other requirements prescribed by National Security Agency. This list is included in the National Security Agency information systems Security Products and Services Catalogue, issued quarterly and available through the Government Printing Office.

Preproduction Model—Version of Information Systems Security equipment that employs standard parts and is suitable for complete evaluation of form, design, and performance. Pre-production models are often referred to as beta models.

Prescribed Form—A form prescribed in a DoD publication. The Office of the Assistant Secretary of Defense approves and mandates their use by the military departments. A standard or specialized Air Force publication prescribes them, except when prescribed in DoD issuances.

Preservation—(1) The provision of adequate facilities to protect, care for, or maintain records. (2) Specific measures, individual and collective, undertaken to maintain, repair, restore, or protect records.

Pretty Good Privacy (PGP)—A software encryption capability distributed on the internet for assuring the privacy of user E-mail messages. PGP uses public key encryption. NOTE**:** All encryption capabilities used by the Air Force must be validated by NIST or, endorsed by NSA, depending on the type of information to be protected prior to use.

Prime Word—A word used in a data element name that represents the data grouping to which the data element belongs.

Printing—Any process that produces multiple copies of printed material. This includes composition, platemaking, press work (includes electronic printing), binding, and microform production. It does not include office photocopying or any other method that is capable of only limited production. Unless designated as a printing plant or duplicating facility, the normal output (6 copies or less) of data processing installation is considered limited production. There are two kinds of Air Force printing: (a) departmental printing which is required throughout the Air Force, and (b) field printing which is done by a major command, field operating agency, or direct reporting unit mainly for its own use.

Prior Master File—A file that was at one time the current master file, but the master file updating process superseded it. Usually second, third, or fourth generation tapes (or other media) reflecting superseded data or a superseded master file that has lost all or some of its data.

Privacy Act Request—An oral or written request by an individual about his or her records in a system of records.

Privacy Protection—Establishment of appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of data records. It also protects both security and confidentiality against anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom such information is maintained.

Private Access Pages—Web pages intended for viewing by a limited audience.

Private Branch Exchange (PBX)—A subscriber-owned telecommunications exchange that usually includes access to the public switched network.

Private Key—A cryptographic key used in the dual key system, uniquely associated with an entity, and not made public; it is used to generate a digital signature. This key is linked mathematically with a corresponding public key.

Private Key—Encryption methodology in which the encryptor and decryptor use the same key, which

must be kept secret.

Private Web Server—In computer networking, a web server designed for and/or provides information resources that are limited to a particular audience, such as the Department of Defense or its components.

Privileged Access—Explicitly authorized access of a specific user, process, or computer to computer resources.

Privileged Data—Data not subject to usual rules because of confidentiality imposed by law, such as chaplain, legal, and medical files.

Procedural Interface Standards—Specifications for exchanging information across an interface. The standards define format, language, syntax, vocabulary, and interface operating procedures. Information exchanged among C4 systems using a tactical digital information link, modulation transfer function, and other combat data links.

Processor—In a computer, a functional unit that interprets and executes instructions.

Product Announcement—In information management, provides customers at all levels with information on changes to the status of publications and forms. Product announcements are issued by the publishing functions at AFDPO, MAJCOMs, NAFs, wings, etc.

Profile—In computing, a set of one or more base standards, and, where applicable, the identification of chosen classes, subsets, options, and parameters of those base standards, necessary for accomplishing a particular function.

Program—In computing, a sequence of instructions used by a computer to perform a particular function or solve a given problem.

Programmable Read-Only Memory (PROM)—In computing, a storage device that, after being written to once, becomes a read-only memory.

Programming Language—An artificial language that is used to generate or express computer programs.

Project Support Agreement (PSA)—A document prepared by the C4 systems program engineer that describes: what equipment to install; sites agreed on; supporting construction; services required; operational, technical, or other constraints affecting a C4 systems requirement; and responsibilities of the host base civil engineer, base C4 systems staff, and other supporting activities.

Prompt—Text or graphic display that indicates the start point for user-generated actions. This term is also used for software-generated instructions for process confirmation.

Propagation of Risk—Spreading of risk in a network when a system with an accepted level of risk is connected to that network.

Propagation—In radio communications, the motion of electromagnetic waves through or along a medium or in a vacuum.

Protected Communications—Telecommunications deriving their protection through use of type 2 products or data encryption standard equipment. See Type 2 Product.

Protected Distribution System (PDS)—Wire line or fiber optic distribution system used to transmit unencrypted classified national security information through an area of lesser classification or control.

Protected Satellite Communications (SATCOM)—The system's ability to avoid, prevent, negate, or mitigate the degradation, disruption, denial, unauthorized access, or exploitation of communications

services by adversaries or the environment.

Protection Equipment—Type 2 product or data encryption standard equipment that the National Security Agency has endorsed to meet applicable standards for the protection of telecommunications or AISs national security information.

Protection Interval (PI)—In high-frequency radio automatic link establishment, the period between changes in the time-of-day portion of the time-varying randomization data used for encrypting transmissions.

Protection Philosophy—Informal description of the overall design of an information system delineating each of the protection mechanisms employed. Combination of formal and informal techniques, appropriate to the evaluation class, used to show the mechanisms are adequate to enforce the security policy.

Protection Ring—One of a hierarchy of privileged modes of an information system that gives certain access rights to user programs and processes that are authorized to operate in a given mode.

Protective Packaging—Packaging techniques for communications security material that discourage penetration, reveal that a penetration has occurred or was attempted, or inhibit viewing or copying of keying material prior to the time it is exposed for use.

Protective Technologies—Special tamper-evident features and materials employed for the purpose of detecting tampering and deterring attempts to compromise, modify, penetrate, extract, or substitute information processing equipment and keying material.

Protocol (Software)—A formal set of conventions or rules that govern the interactions of processes or applications within a computer system or network. Also, a set of rules that govern the operation of functional units to achieve communication.

Protocol—In data communications, (1) a set of rules governing network functionality (the open system interconnection reference model uses sets of communication protocols to facilitate communications between computer networks and their components); (2) a formally specified set of conventions governing the format and control of inputs and outputs between two communicating systems; (3) A set of rules and formats, semantic and syntactic, that establish the method by which data is exchanged over the Internet.

Protonic Memory—In computer technology, protonic memory uses protons rather than electrons in memory retentive chips to achieve non-volatile memory.

Provisioning—(1) In acquisition logistics, the management process of determining and acquiring the range and quantity of support items necessary to operate and maintain an end item of materiel for an initial period of service (until the normal demand-based replenishment processes can provide support). (2) In networking, the establishment, operations, and maintenance of voice, data, video transmissions, and other services on a network in such a way as to provide end-to-end services to the user.

Proxy Cache—In networking, an application-layer network service for caching web objects. A type of shared cache, proxy caches can be accessed and shared simultaneously by many users. Proxy cache reduces the amount of bandwidth used by large corporation and Internet Service Providers. Proxy caches often operate on dedicated hardware and operate much like other network services, such as e-mail, web serves, etc.

Pseudorandom Noise—Noise that satisfies one or more of the standard tests for statistical randomness. Although it seems to lack any definite pattern, there is a sequence of pulses that repeat after a very long

time interval.

Psophometer—In telecommunications, a noise measuring set; an instrument that measures circuit noise voltages. The psophometer is widely used in Europe and is calibrated with a tone of 800 Hz, 0 dBm, instead of the more commonly used test tone of 1 kHz in the US..

Psychological Operations (PSYOP)—Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning and, ultimately, the behavior of foreign governments, organizations, groups, and individuals. The purpose of PSYOP is to induce or influence foreign attitudes and behavior favorable to the originator's objectives.

Public Access Pages—Air Force web pages intended for viewing by the general public. Information on these pages should be of interest to the general public.

Public Cryptography—Body of cryptographic and related knowledge, study, techniques, and applications that is, or intended to be, in the public domain.

Public Dissemination Products (PDP)—Information products produced by the Air Force specifically for dissemination to the general public.

Public Domain Software—Software released to the general public for use without payment or restriction. Generally, no support or software accuracy is promised.

Public Information—Any information, regardless of form or format, that an agency discloses, disseminates, or makes available to the public.

Public Key—A cryptographic key used in the dual key system, uniquely associated with an entity, and not made public; it is used to generate a digital signature. This key is linked mathematically with a corresponding private key.

Public Key Certificate—Contains the name of a user, the public key component of the user, and the name of the issuer who vouchers that the public key component is bound to the named user.

Public Key Cryptography (PKC)—Encryption system that uses a linked pair of keys. What one pair of keys encrypts, the other pair decrypts.

Public Key Encryption—A form of encryption that utilizes a unique pair of keys, one, the "public key," being openly known, and the other, the "private key," being known only to the recipient of an encrypted message. At the recipient's discretion, the public key is made available to those who may have occasion to send an encrypted message to that recipient. The sender uses the recipient's public key to encrypt a message. The encrypted message, which cannot be decrypted by means of the public key, is then delivered by conventional means to the recipient, who uses the matching private key to decrypt the message. Users of public-key encryption systems may register their public keys in several public databases.

Public Key Infrastructure—In data communications, the methodology that allows business to be conducted electronically with the confidence that (1) the person sending the transaction is actually the originator, (2) the person receiving the transaction is the intended recipient, and (3) data integrity has been maintained.

Public Switched Telephone Network (PSTN)—The regular (old-fashioned) telephone system.

Publication—An officially produced, published, and distributed document issued for compliance, implementation, and/or information.

Published—Fully coordinated, certified, and authenticated manuscripts that were processed through the

publishing management office, announced in the Product Announcement, posted, and made accessible via the official publications and forms World Wide Web (WWW) site, or printed, if applicable. Once posted, manuscripts are official documents.

Publishing—The process for creating and distributing information through officially sanctioned parameters and procedures as described in the Air Force publications management program via AFI 33-360, Volume 1. Publishing includes the process of creating and distributing instructions, manuals, etc.

Pull-Down Menu—In computing, a list of options attached to a selection on a menu bar which are tailored to the needs of each program.

Pulse Amplitude Modulation (PAM)—That form of modulation in which the amplitude of the pulse carrier is varied in accordance with some characteristics of the modulating signal.

Pulse Code Modulation (PCM)—In telecommunications, that form of modulation in which the modulating signal is sampled, the sample quantized and coded, so that each element of information consists of different kinds of numbers of pulses and spaces.

Pulse Duration Modulation (PDM)—In telecommunications, that form of modulation in which the duration of a pulse is varied in accordance with some characteristic of the modulating signal.

Pulse Position Modulation (PPM)—In telecommunications, that form of modulation in which the positions in time of the pulses are varied in accordance with some characteristic of the modulating signal without modifying the pulse width.

Pulse Recurrence Interval (PRI)—In radar, the time interval between the start of a transmitted pulse and the start of the next pulse. PRI is the reciprocal of the pulse recurrence frequency.

Pulse Repetition Frequency (PRF)—In radar, the rate, usually given in hertz or pulses per second, at which a pulse or pulsegroup is transmitted.

Purging—(1) Rendering stored information unrecoverable by laboratory attack. (2) The removal of data from an information system and its storage media in such a way as to provide assurance that the data is unrecoverable by technical means. Purging is the first step in removing classification from media. The other two steps are review of the media, and administrative removal of security classification markings and controls.

Push Technology—Push or webcasting technology is a software approach for the automatic distribution of pre-selected categories of information, such as news articles, to internet and intranet users. Push technologies create automated intelligent relationships between information publishers and subscriber channels. Push technology is a direct contrast to the “pull” method of viewing information on the World Wide Web.

Quadbit—In data communications, four bits that are transmitted in a single baud.

Quadded Cable—A cable formed by taking four, or multiples of four, paired and separately insulated wires and twisting these together within an overall jacket.

Quadrant—Short name referring to technology that provides tamper-resistant protection to cryptoequipment.

Quadrature—(1) The state of being separated in phase by 90 degrees. (2) Pertaining to the phase relationship between two periodic quantities varying with the same period (that is, the same frequency or repetition rate), when the phase difference between them is one-quarter of their period.

Quadrature Amplitude Modulation (QAM)—In data communications, a method of converting digital signals into analog signals for transmission over a telephone network. It combines both amplitude and phase modulation techniques.

Quadrature Phase Shift Keying (QPSK)—A digital frequency modulation technique used for sending data over coaxial cable networks. Because QPSK is easy to implement and is fairly resistant to noise, it is used primarily for sending data from the cable subscriber upstream to the Internet. QPSK is a phase shifting or modulating technique which uses four different phase angles which are shifted or separated by 90 degrees, hence its name.

Quadruple Diversity—In radio communications, the term applied to the simultaneous combining of, or selection from, four independently fading radio signals and their detection through the use of space, frequency, angle, time, or polarization characteristics or combinations thereof. Diversity reception is used to minimize the effects of fading.

Qualitative Data—A data value that is a non-numeric description of a person, place, thing, event, activity, or concept.

Quantitative Data—A numerical expression that uses Arabic numbers upon which mathematical operations can be performed.

Quantization—In time division multiplexing, a process in which the continuous range of values of a signal is divided into non-overlapping, but not necessarily equal subranges, and to each subrange a discrete value of the output is uniquely assigned. Whenever the signal value falls within a given subrange, the output has the corresponding discrete value.

Quantizing Noise—In time division multiplexing, an undesirable random signal caused by the error of approximation in a quantizing process and which manifests itself as a background noise on a telecommunications channel. It is solely dependent on the particular quantization process used and the statistical characteristics of the quantized signal.

Quasi-Analog Signal—A digital signal that has been converted to a form suitable for transmission over a specified analog channel.

Quick-Fix Phase—One of several phases of the C4I for the Warrior concept. The quick-fix phase includes the six years of the program objective memorandum development and acquisition cycle. This phase is used to resolve current critical C4I interoperability problems.

Rack—In communications-electronics, pertaining to a vertical, metal frame or chassis on which panels or items of electrical or electronic equipment are mounted. A standard rack is 19 inches wide.

Radar Baseline Evaluation—An evaluation to optimally configure the radar system and determine its capabilities and limitations.

Radar Coverage Indicator (RCI)—A specialized vertical radar coverage diagram used to estimate the radar set's capability to detect known radar cross section targets by range and altitude.

Radar Cross Section (RCS)—A measure of the portion of the incident energy reflected from a target back to the radar set, normally expressed in decibel (dB) units relative to a reference.

Radiating Element—In radio communications, that part of a transmitting antenna or antenna system from which the electromagnetic energy is radiated directly. Also referred to as the active element.

Radiation—(1) In radio communications, the planned emission of energy in the form of electromagnetic

waves. (2) The outward flow of energy from any source in the form of electromagnetic waves.

Radiation Hazards (RADHAZ)—In communications, electromagnetic radiation hazards and concerns about the effects on the human body of non-ionizing radiation caused by exposure to high-power transmitters or electronic equipment that produces x-rays.

Radiation Pattern—The variation of the field intensity of electromagnetic energy radiated from an antenna as a function of direction. The radiation pattern of an antenna for a given frequency or range of frequencies is the same whether transmitting or receiving.

Radio—A general term applied to the use of radio waves as a method of communicating over a distance by modulating electronic signals and radiating these signals as electromagnetic waves.

Radio Astronomy—Astronomy based on the reception of radio waves of cosmic origin.

Radio Channel—An assigned band of frequencies used for radio communications. The channel is normally identified by a predetermined letter, number, or code word in reference to its specific frequencies.

Radio Communications—A form of communication involving the transmission and reception of electromagnetic waves through the atmosphere or in space. Information is conveyed typically by modulation of the carrier or center frequency of the radio signal. There are a number of varied and different modulation techniques.

Radio Day (RAYDAY)—A telecommunications term used to represent message creation and station log entry dates. RAYDAYS are numbered sequentially from the first day of January (001 for 1 January, 002 for 2 January, etc.). Each RAYDAY begins at 0000 Greenwich mean time.

Radio Frequency (RF)—Any frequency suitable for radio transmission.

Radio Frequency Bandwidth—The difference between the highest and lowest emission frequencies in the region of the carrier or principal carrier frequency.

Radio Frequency Interference (RFI)—A manmade or natural, intentional or unintentional, electromagnetic propagation that results in unintentional and undesirable responses from, or performance degradation or malfunction of, electronic equipment.

Radio Frequency Spectrum—The frequencies or wavelengths associated with radio wave propagation ranging from 3 kHz to 3,000 GHz or in wavelengths (or from 100 kilometers to 0.1 millimeter in length).

Radio Horizon—The locus of the points at which direct waves from an antenna become tangential to the earth's surface. Near the surface of the earth, the radio horizon generally extends beyond the earth horizon due to atmospheric and other influences on the radio waves.

Radio Relay—The transmission and reception of radio signals between stations of a terrestrial point-to-point radio communications system. Radio relay links may form part of the connection between a satellite earth station and switching centers.

Radio Repeater (Station)—In radio communications, a station in a radio relay system whose equipment is in a special back-to-back configuration that retransmits all communications entering its receivers.

Radio Wave—An electromagnetic wave of a frequency arbitrarily lower than 3000 GHz. Synonym: Hertzian Wave.

Random Access Memory (RAM)—Computer memory that stores and recalls information in any order

or sequence. This type of memory is used for temporary storage. RAM requires electrical power to remember information; all information in RAM is lost when the electrical power to the unit is turned off.

Random Errors—In data communications, errors distributed over the signal in time so that they can be considered statistically independent from each other.

Random Noise—In telecommunications, system or circuit noise consisting of a large number of random transient disturbances that is unpredictable except by statistical means.

Randomizer—(1) An electronic device used to invert the sense of pseudorandomly selected bits of a bit stream to avoid long sequences of bits of the same sense. (2) Analog or digital source of unpredictable, unbiased, and usually independent bits. Randomizers can be used for several different functions, including key generation or to provide a starting state for a key generator.

Reachback—(1) The process by which forward-deployed units obtain materiel, services, and/or information from organizations that are not forward-deployed. Reachback provides combat support and/ or informational support from a rear area or out-of-theater to in-theater units. (2) A satellite link from a deployed location to a standard tactical entry point site or a link to the home station via the global grid.

Read-Only Memory (ROM)—A computer memory that stores permanent information. This information is constant and cannot be erased or changed, even when the electrical power to the unit is turned off. All personal computers contain programs in ROM that execute when the computer is turned on.

Real Time—Pertaining to the timeliness of data or information that has been delayed only by the time required for electronic communication. This implies that there are no noticeable delays.

Real-Time Processing—A form of processing that controls an environment by receiving data, processing it, and taking action to return results in time to affect the functioning of the environment at that time.

Received Signal Level (RSL)—The value of a specified bandwidth of signals at the receiver radio frequency input terminals relative to an established reference.

Recognition Memory (REM)—In character recognition, a read-only memory in the optical character reader holding the bit patterns of characters in the font. This data is pattern matched with the corresponding information from the input character.

Records—According to 44 U.S.C. 3301, the term "records" includes all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, that are: (1) made or received by an agency of the United States Government under Federal Law or in connection with the transaction of public business; and (2) preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them.

Rectangular Waveguide—In radio communications, a waveguide of rectangular cross-section used for the transmission of radio frequency signals over relatively short distances (for example, between the transmitter or receiver and the antenna).

RED Key—Unencrypted key. See BLACK Key.

RED Line—Any line in which classified or unenciphered signals are carried.

RED Signal—Any electronic emission (e.g., plain text, key, key stream, subkey stream, initial fill, or control signal) that would divulge national security information if recovered.

RED Switch—A voice telephone switching system designed and installed to allow for processing RED (unencrypted) secure conversations. The system has adequate isolation between channels to prevent crosstalk. The distribution system provides adequate shielding ensuring radiation of RED data does not occur. The design allows no multiple-party access without the knowledge of the principal users. Subscribers are placed in and out of service when station equipment is not under the scrutiny of properly cleared persons. **RED Switch** interfaces provide encryption and allow subscribers access to other secure networks.

RED/BLACK Concept—Separation of electrical and electronic circuits, components, equipment, and systems that handle national security information (RED), in electrical form, from those which handle non-national security information (BLACK) in the same form.

RED/BLACK Concept—The concept where the electrical and electronic circuits, components, equipment, and systems, which handle plain language information in electric signal form (RED) are separated from those which handle encrypted or unclassified information (BLACK). Under this concept, RED and BLACK terminology is used to clarify specific criteria relating to, and to differentiate between such circuits, components, equipment, and systems, and the areas in which they are located.

RED—Designation applied to information systems, and associated areas, circuits, components, and equipment in which national security information is being processed.

Reference Antenna—An antenna that may be real, virtual, or theoretical, and has a radiation pattern that can be used as a basis of comparison with other antenna radiation patterns.

Reference Circuit—In electronics, a hypothetical circuit of specified length and configuration with defined transmission characteristics primarily used as a reference for the performance of other circuits and as a guide for planning and engineering circuits and networks.

Reference Frequency—A frequency having a fixed and specific position with respect to the assigned frequency. The displacement of this frequency with respect to the assigned frequency has the same absolute value and sign that the displacement of the characteristic frequency has with respect to the center of the frequency band occupied by the emission. Also see: Characteristic Frequency.

Reference Monitor—Access control concept that refers to an abstract machine that mediates all accesses to objects by subjects.

Reference Validation Mechanism—Portion of a trusted computing base whose normal function is to control access between subjects and objects, and whose correct operation is essential to the protection of data in the system.

Reflective Array Antenna—.—An antenna system, such as a billboard antenna, in which the driven elements are situated at a predetermined distance from a surface designed to reflect the signal in a desired direction.

Reflector—In radio communications, one or more conductors or conducting surfaces for reflecting radiant energy, such as part of an antenna system.

Refraction—The natural phenomenon of the bending of a radio or lightwave as it passes obliquely from one medium to another medium of a different density.

Regenerative Feedback—In an electronic device or circuit, feedback in which the portion of the output signal that is returned to the input of the device has a component that is in phase with the input signal.

Regenerative Repeater—An electronic device in which the received pulse signals are amplified, reshaped, retimed, and transmitted to the next destination. Synonym: Regenerator.

Register—A memory device, usually high speed, for the temporary storage of one or more words to facilitate arithmetical, logical, or transferal operations.

Registration Authority—A person or organization having authority over a portion of the directory information tree.

Release Prefix—Prefix appended to the short title of United States produced keying material to indicate its foreign releasability. "A" designates material that is releasable to specific allied nations and "U.S." designates material intended exclusively for United States use.

Reliability—The probability that an item (C4 system, equipment, assembly, or component) will perform its intended function for a specified interval under stated conditions. The overall reliability of a system is measured in terms of the mean time between failure, and mean time to repair.

Remanence—Residual information that remains on storage media after clearing. See magnetic remanence and clearing.

Remote Database Access (RDA)—The interconnecting of database applications among heterogeneous environments by providing standard open system interconnection application protocols to establish a remote connection between database client and database server.

Remote Rekeying—Procedure by which a distant cryptoequipment is rekeyed electrically. See Automatic Remote Rekeying and Manual Remote Rekeying.

Remote Switching Terminal—In telecommunications, an electronic remote switch placed at a subordinate wire center for subscriber lines and normally considered a part of the main switching equipment. A concentrator installed at a remote location to reduce the number of trunks needed to connect remote subscribers to the main switching equipment may serve the same purpose. It may rely on the main telephone system for processor control supervision, trunking, and operator assistance.

Remote Switching Unit (RSU)—In telecommunications, a part of an electronic switch located separate from the main switch. It receives its commands from the parent switch but is capable of connecting local users to each other without the need to route them through the parent switch. This limits the number of connections between the local area and the parent switch. A subscriber of an RSU can have all of the features available to a direct subscriber of the parent switch.

Reorder Point—The point at which a stock replenishment requisition would be submitted to maintain the predetermined or calculated stock objective.

Repair Parts—Consumable bits and pieces, i.e., individual parts or nonreparable assemblies, required for the repair of end items and spares. Repair parts are not normally subject to repair and are generally discarded on failure.

Report Control Symbol (RCS)—A standard agency designation (control number) for a report consisting of letters or numbers indicating that the report has been reviewed and approved according to DoD and Air Force-directed procedures.

Reprographics—Duplicating, copying, micrographics, and related processes.

Repudiation—The denial by a message originator or recipient that a message was sent or received. In the Defense Message System, the message signature ensures that an originator cannot repudiate the message.

Requirement—The need of an operational user, initially expressed in broad operational capability terms and in the format of a Mission Need Statement (MNS), for a new or improved capability which, when satisfied, will result in an increase in the probability of operational mission success or a decrease in the cost of mission support.

Requirements Process—A three-step process that identifies C4 systems requirements, develops a certified technical solution, and allocates resources.

Requisition (Publications/Forms)—A demand or request for publications or forms. Unlike a requirement, a requisition is an order for the actual material. Often requisitions and requirements are submitted at the same time for a publication. Forms are only requisitioned and may never be put on requirement.

Residue—(1) Data left in storage after information processing operations are complete, but before degaussing or overwriting has taken place. (2) Data left in storage after automated information processing operations are complete, but before degaussing or overwriting has taken place.

Resource Encapsulation—Method by which the reference monitor mediates accesses to an information system resource. Resource is protected and not directly accessible by a subject. Satisfies requirement for accurate auditing of resource usage.

Resource—Any function, device, or data collection that may be allocated to users or programs (i.e., memory, tape drives, disk space, and so forth).

Retrograde Orbit—Of a satellite orbiting the earth, an orbit in which the projection of the satellite's position of the (earth's) equatorial plane revolved in the direction opposite that of the rotation of the earth.

Return Loss—The ratio, at the junction of a transmission line and a terminating impedance, of the reflected wave to the incident wave, expressed in decibels. More broadly, Return Loss is the loss in power experienced by an electrical signal and is a measure of the dissimilarity between two impedances.

Return-to-Zero (RZ) Code—A code form having two information states called zero and one, and having a third state or condition to which each signal returns during each period. See also Non-Return-to-Zero Code.

Reverse Address Resolution Protocol (RARP)—A protocol for a physical machine in a local area network to learn its internet protocol (IP) address from a gateway server's address resolution protocol table or cache.

Reverse Engineering—The inference and documentation, to a specified level of detail and business generalization, of models of data and information structures, and business rules underlying one or more current or proposed data processing systems.

Rhombic Antenna—A long-wire antenna used in high frequency (HF) radio communications and noted for its high efficiency. The antenna is composed of long-wire radiators comprising the side of a rhombus, hence its name. Its disadvantage is the relatively large ground area required because of its size.

Ribbon Cable—(1) Any cable constructed as a ribbon with parallel elements. (2) A fiber optic cable in which the optical fibers are held in grooves and laminated within a flat semi-rigid strip of material, such as plastic, that positions, holds, and protects them.

Ring Latency—In a computer ring network, such as a token ring, the time required for a signal to propagate once around the ring.

Risk Analysis—An analysis of system assets and vulnerabilities to establish an expected loss from test findings and analysis of system documentation (i.e., Trusted Facility Manual , Security Features Users Guide, System Security Architecture, etc.). The purpose of a risk analysis is to determine if countermeasures are adequate to reduce the probability of loss or the impact of loss to an acceptable level.

Risk Assessment—Process of analyzing threats to and vulnerabilities of an Information System, and the potential impact that the loss of information or capabilities of a system would have on national security and using the analysis as a basis for identifying appropriate and cost-effective counter-measures.

Risk Index—Difference between the minimum clearance or authorization of information system users and the maximum sensitivity (e.g., classification and categories) of data processed by the system.

Risk—Probability that a particular threat will exploit a particular vulnerability of the system.

Round Trip—In satellite communications, the distance from a transmitting ground station through the satellite to a receiving ground station and return via the satellite to the originating station. This distance is used to compute round trip delay time.

Route—(1) In telecommunications system operations, the geographical path of a circuit in establishing a chain of connections. (2) To construct the path a circuit is to take in a communications network going from one station to another or from source to destination.

Router—In data communications, a device used to interconnect two or more networks. Routers operate at the network layer (layer 3) of the open system interconnection reference model. A typical application is to allow a number of machines to access the Internet using a single IP address. The router moves network traffic from the internet to a LAN.

Routine Use—A disclosure of records to individuals or agencies outside DoD for a use that is compatible with the purpose for which the Air Force created the records.

Rubidium Clock—A clock containing a quartz oscillator stabilized by a rubidium standard.

Rubidium Standard—A frequency standard in which a specified hyperfine transition of electrons in rubidium-87 atoms is used to control the output frequency. A rubidium standard consists of a gas cell through which an optical signal is passed. The gas cell has inherent inaccuracies that relegate the rubidium standard to its status as a secondary standard.

Safeguarded Forms—Blank forms that could be put to fraudulent use, but not to a degree requiring complete accountability. Such forms are stored in locked cabinets, secure filing cabinets, or locked rooms.

Sample Key—Key intended for off-the-air demonstration use only.

Sanitizing—The removal of information from AIS storage media such that data recovery using known techniques or analysis is prevented. Sanitizing includes the removal of data from the media (purging), verification of the purging action, and removal of all classification labels and markings. Properly sanitized media may be subsequently declassified upon observing the organization's respective verification and review procedures.

Satellite Access—In satellite communications, the establishment of contact with a communications satellite in space or orbiting the earth.

Satellite Communications Control Plan—A master plan that provides information for the operational benefit of all users of a particular space segment, and which describes the control exercised by a master communications station to ensure that all units of the associated earth segment operate within their

assigned parameters and according to prescribed procedures.

Satellite Control—Action by a satellite ground control station involving station keeping, stabilization, maneuvering and repositioning, commanding, anomaly resolution, tracking, telemetry, and ephemeris generation of a satellite.

Satellite Earth Terminal—A ground communications facility, part of a satellite communications link, that processes, transmits, and receives communications signals between the earth and the satellite.

Satellite Link—In satellite communications, a radio link between a transmitting earth station and a receiving earth station through one satellite. A satellite link comprises one uplink and one downlink.

Satellite—An object or vehicle orbiting, or intended to orbit, the earth, moon, or other celestial body.

Saturation—In a communications system, the condition in which a component of the system has reached its maximum traffic handling capacity.

S-Band—In radio communications, the frequency range of 2-4 gigahertz.

Scalability—(1) The ability to use the same application software on many different classes of hardware/software platforms from personal computers to supercomputers (extends the portability concept); the capability to grow to accommodate increased workloads. (2) The ease with which software can be transformed from one graduated series of application platforms to another.

Scatter—The process where the direction, frequency, or polarization of electromagnetic (radio) waves are changed when the waves encounter one or more discontinuities in the medium that have lengths on the order of a wavelength. See: Ionospheric Scatter and Tropospheric Scatter.

Scavenging—Searching through object residue to acquire data.

Scientific and Technical Information (STINFO)—All technical publications and documents generated by Air Force-funded research, development, test, and evaluation (RDT&E) programs, including working papers, memoranda, and preliminary reports that the DoD could decide to disseminate to the public domain.

Scintillations—In radio communications, rapid fluctuations in the strength of the (received) radio frequency signal due to atmospheric, manmade, or natural interferences or effects.

Scratch Pad Store (SPS)—Temporary key storage in cryptoequipment.

Screen—The face of a video display tube that displays an image or data.

Seamless C4 Environment—In communications, an electronic environment that allows data to be accessed by the warfighter without regard to physical or electronic boundaries.

Seamless Operations—End-to-end automation and procedures that integrate all command, control, communications, computers and intelligence (C4I) elements and networks into an interoperable and cohesive global network that is transparent to the warrior.

Search Engine—A tool used to search the Internet for a particular subject or topic.

Secondary Channel—In a system in which two channels share a common interface, a channel that has a lower data signaling rate capacity than the primary channel.

Secondary Frequency Standard—A frequency standard that does not have inherent accuracy, and therefore must be calibrated against a primary frequency standard. (Secondary standards include crystal

oscillators and rubidium standards.)

Secure Configuration Management—Procedures appropriate for controlling changes to a system's hardware and software structure to make sure changes will not lead to violations of the system's security policy.

Secure Sockets Layer (SSL)—A security protocol that provides privacy over the Internet. The protocol allows client/server applications to communicate, while preventing eavesdropping. Servers are always authenticated and clients are optionally authenticated.

Secure State—Condition in which no subject can access any object in an unauthorized manner.

Security Architecture—Detailed description of all aspects of the system that relate to security, along with a set of principles to guide the design.

Security CONOPS—A high-level description of how the security of the system operates and a general description of the security characteristics of the system, such as user clearances, data sensitivity, and data flows.

Security Critical Mechanisms—Security mechanisms whose correct operation is necessary to ensure that the security policy is enforced.

Security Domains (Class B3)—Advanced trusted computing base that provides highly effective and mandatory access controls. Significant security and software engineering must be accomplished during the design, implementation, and testing phases to achieve the required level of confidence, or trust. Operational support features extend auditing capabilities as well as other functions needed for a trusted system recovery.

Security Fault Analysis—Assessment, usually performed on information system hardware, to determine the security properties of a device when hardware fault is encountered.

Security Features Users Guide (SFUG)—Guide or manual that explains how the security mechanisms in a specific system work.

Security Label—Information that represents the sensitivity of a subject or object, such as its hierarchical classification (CONFIDENTIAL, SECRET, TOP SECRET) together with any applicable nonhierarchical security categories (e.g., sensitive compartmented information, critical nuclear weapon design information).

Security Level—Combination of classification levels and a set of categories, including sensitive unclassified categories, that represents the sensitivity of the information.

Security Measures—The means to protect and defend information and information systems. Security measures include operations security and information assurance.

Security Mode of Operation—Description of the conditions under which an information system operates, based on the sensitivity of information processed and the clearance levels, formal access approvals, and need to know of its users. Four modes of operation are authorized for processing or transmitting information: dedicated mode, system-high mode, compartmented/partitioned mode, and multilevel mode.

Seed Key—Initial key used to start an updating or key generation process.

Seepage—Accidental flow of data to unauthorized individuals, access to which is presumed to be controlled by computer security safeguards.

Self-Authentication—Implicit authentication, to a predetermined level, of all transmissions on a secure communications system.

Semiconductor—A material (element or compound) that displays a different electrical resistance in opposite directions of current flow. It has a higher resistivity than a conductor, but a lower resistivity than an insulator. Semiconductor materials are the basis of diodes, transistors, thyristors, photodiodes and integrated circuits.

Semi-Duplex—A method of operating a communications circuit where one end operates in the duplex mode and the other end in the simplex mode. Sometimes used in mobile systems with the base station being duplex and the mobile station being simplex.

Sensitive Compartmented Information (SCI)—Security classification that includes only that intelligence material having special controls indicating restrictive handling for which systems of compartmentation of handling are formally established,

Sensitive Information—Information, the loss, misuse, or unauthorized access to or modification of, which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (Systems that are not national security systems, but contain sensitive information are to be protected according to the requirements of the Title 40 U.S.C. 759, *Computer Security Act of 1987*.)

Sensitive—Requiring special protection from disclosure that could cause embarrassment, compromise, or threat to the security of the sponsoring power. May be applied to an agency, installation, person, position, document, material, or activity sensitive compartmented information. All information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. (These controls are over and above the provisions of DoD Regulation 5200.1.)

Sensitivity And Criticality Assessment—Study to determine the value of a computer system by taking into account the cost, capability, and jeopardy to mission accomplishment or human life associated with the system.

Sensitivity—In a radio receiver, the minimum input signal required to produce a specified output signal having a specified signal-to-noise ratio.

Serial Line Internet Protocol (SLIP)—Similar to Point-to-Point Protocol (PPP). SLIP is another standard protocol used to run TCP/IP over serial lines, such as telephone circuits or RS-232 cables. Unlike PPP, SLIP does not work on a LAN connection. SLIP is a popular way for dial-up users to access the Internet over conventional telephone lines.

Serial Transmission—The transmission in a sequence, over a single line, of individual signal elements. The sequential elements may be transmitted with or without interruption, provided they are not transmitted simultaneously.

Serial—The handling of one item after another in a single facility such as transfer or store in a digit-by-digit time sequence or to process a sequence of instructions one at a time.

Service Provider (Global Information Grid [GIG])—Any type of organization internal or external to

the DoD and that has designated responsibility for the operation of one or more of the GIG computing and communications assets.

Service Software—In computer programming, software designed specifically for service and repair work.

Shaping Network—A network inserted in a circuit for improving the wave shape of the signals.

Shared Data Field—A field contained within a record, defined to occupy the same record positions with more than one data element.

Shareware—Privately or commercially developed software that is normally distributed free of charge but a fee is generally expected for continued or extended use. Normally, implied or promised support by the author is minimal or nonexistent.

Shell—An outer layer of an operating system that provides a menu-driven or graphical user interface, or the user's way of commanding the computer. Instead of presenting the user with a command line prompt, the shell presents a list of programs from which the user can choose.

Shift Register—In computing, a storage device, usually in a central processing unit, in which device a serially ordered set of data may be moved, as a unit, into a discrete number of storage locations.

Ship Earth Station—A mobile satellite earth station in the maritime mobile satellite service located onboard ship.

Short Title—(1) Identifying combination of letters and numbers assigned to certain COMSEC materials to facilitate handling, accounting, and control. (2) A short, identifying combination of letters, and/or numbers assigned to a document or device for purposes of brevity and/or security.

Shortwave (Radio)—Pertaining to radio waves with a frequency above the medium frequency range (above 3 MHz), corresponding to wavelengths that are less than 100 meters. The term shortwave is not a precise term and is not officially recognized by the international community. It is generally associated with operations in the High Frequency band (3-30 MHz)

Side Lobe—In a directional antenna radiation pattern, a lobe in any direction other than that of the main lobe.

Sideband Transmission—That method of transmission in which frequencies produced by amplitude modulation occur above and below the carrier frequency. The frequencies above (higher than) the carrier are called upper sideband; those below (lower than) the carrier are called lower sideband. The two sidebands may carry the same or different information. The carrier and either sideband may be suppressed independently. In conventional amplitude modulation both sidebands carry the same information and the carrier is present.

Sideband—In radio communications, a band of frequencies of a transmitted (radio frequency) signal above and below the carrier frequency, produced by the modulation process.

Sidetone—In telephone communications, the sound of the speaker's own voice (and background noise) as heard in the speaker's telephone receiver.

Signal Compression—In analog (usually audio) communications systems, the reduction of the dynamic range of a signal by controlling it as a function of the inverse relationship of its instantaneous value relative to a specified reference level. Signal compression is used, amongst others, to improve signal-to-noise ratios, prevent overload of succeeding elements of a system, or to match the dynamic

ranges of two devices.

Signal—(1) As applied to electronics, any transmitted electrical impulse. (2) Operationally, a type of message, the text of which consists of one or more letters, words, characters, signal flags, visual displays or special sounds with pre-arranged meaning, and which is conveyed or transmitted by visual, acoustical, or electrical means. (3) Detectable transmitted energy that can be used to carry information.

Signaling—(1) The use of signals for communication. (2) The method of conveying signals over a circuit. (3) The exchange of information (other than by speech) specifically concerned with the establishment and control of connections and management in a communications network.

Signal-To-Noise (S/N) Ratio—(1) The ratio of the amplitude of the desired signal to the amplitude of the (unwanted) noise signals at a given point in time, expressed in decibels. (2) The amount by which a signal exceeds the circuit noise on a line over which it is transmitted.

Signature Facsimile—A stamp that duplicates an original signature and has the same authority as the original signature.

Significant Modification—In information assurance, any modification to an automated information system or facility that affects the accredited safeguards or results in changes to the prescribed security requirements.

Simple Mail Transfer Protocol (SMTP)—In computer networking, the main protocol used to send electronic mail on the Internet.

Simple Network Management Protocol—In computer networking, a set of standards for communication with devices such as routers, bus, and switches, connected to a Transmission Control Protocol/Internet Protocol (TCP/IP)network.

Simple Object Access Protocol (SOAP)—An Extensible Markup Language (XML)-based interoperability protocol that links applications and services together via the Internet, regardless of operating system, object model, or programming language.

Simple Security Property—The Bell-La Padula security model rule allowing a subject read access to an object only if the security level of the subject dominates the security level of the object.

Simplex Circuit—A circuit affording communications in either direction, but only in one direction at a time and using a ground return path. The circuit may be a single wire with ground return, or may be derived from the center of a balanced two-wire circuit and ground return.

Simplex Operation—The type of operation that permits the transmission of signals over a communications circuit in either direction alternately.

Simulation—The representation of selected characteristics of the behavior of one physical or abstract system by another system. In a digital computer system, simulation is done by software; for example, (a) the representation of physical phenomena by means of operations performed by a computer system, and (b) the representation of operations of a computer system by those of another computer system.

Simultaneous Access—The process of obtaining information from or placing information into storage where the time required for such access depends on the simultaneous transfer of all elements of a word given storage location.

Singing—In telecommunications, an undesired, self-sustaining audio oscillation in a circuit, usually caused by excessive gain in the circuit, unbalance of the hybrid termination, or combination thereof.

Single Sideband (SSB) Transmission—A transmission where only one sideband is transmitted, but the carrier frequency is present.

Single Sideband Suppressed Carrier (SSB-SC) Transmission—A generally amplitude modulated radio signal consisting of one sideband only (upper or lower) and in which the carrier frequency also has been suppressed (filtered out) to the point where it is insufficient to be demodulated in the receiver.

Single-Level Device—Information system device not trusted to properly maintain and separate data to different security levels.

Single-mode Fiber—Fiber-optic cabling with a narrow core that allows light to enter only at a single angle. This cabling has a higher bandwidth than multi-mode fiber, but requires a light source with a narrow spectral width, such as a laser. Also called mono-mode fiber

Site License Agreement—A contractual agreement with a commercial software business allowing use of their software product at a specific site or by a specific group of users. Contracts typically provide free or inexpensive upgrades and allow sharing software with multiple users at less cost than buying individual copies.

Site Preparation—Site preparation of a communications facility includes modifying facilities, surveying sites, and determining allied support costs.

Skip Distance—In radio transmissions, the minimum distance between the transmitting station and the point of return to the earth of the transmitted wave reflected from the ionosphere.

Skip Zone—A roughly coned-shaped region within the transmission range where signals from a transmitter are not received. It is the area between the farthest points reached by the ground wave and nearest points at which the refracted sky waves come back to earth.

Sky Wave—A transmitted radio wave that travels upward from the antenna. Depending on its frequency, a sky wave may be reflected back to earth by the ionosphere.

Slot Antenna—A radiating element formed by a slot in a conducting surface or in the wall of a waveguide.

Small Computer—A data processing system which can execute various programs. It usually consists of a keyboard, peripheral storage device, visual display device, printer, and central processing unit with random-access and read-only memory. A small computer may be operated stand-alone or networked with other computers. Personal computers, microcomputers, text processors, intelligent typewriters, and portable computers are all examples of small computers.

Sniffer—Software tool that audits and identifies network traffic packets.

Soft Keys—Visual representation of key functions on a display screen. This is usually associated with software controlled function key capabilities.

Soft Metric—Metric equivalents calculated by mathematical conversion of inch-pound measurements for specifications, standards, supplies, and services. The physical dimensions are not changed.

Software—A set of computer programs, procedures, and associated documentation concerned with the operation of a data processing system (for example, compilers, library routines, manuals, and circuit diagrams).

Software Domain—A distinct functional area that can be supported by a class of software systems with similar requirements and capabilities. A domain may exist before there are software systems to support it.

Software Engineering—The discipline devoted to the design, development, and use of software.

Software Failure—The inability, due to a fault in the software, to perform an intended logical operation in the presence of the specified/data environment.

Software-intensive System—A system in which software represents the largest segment in one or more of the following criteria: system development cost, system development risk, system functionality, or development time.

Software Maintainability—The probability that the software can be retained in or restored to a specified status in a prescribed period compatible with mission requirements.

Software Portability—The ease with which software can be transferred from one information system to another.

Software Reliability—The probability that the software will perform the intended logical operations for the prescribed missions and periods in the specified data/environment, without failure.

Software Reuse—The process of implementing or updating software systems using existing software assets.

Software Support—The sum of all activities that take place to ensure that implemented and fielded software continues to fully support the operational mission of the system. Software support includes pre- and post-deployment support.

Source Agency—A Federal, state, or local government agency that discloses records for the purpose of a computer match.

Source Code—A file of high-order or assembly language statements, usually containing comments and easily readable steps, which will be compiled or assembled to produce object code for a computer to execute. Modification and debugging of programs are done on source code.

Space Diversity—In radio communications, a method of transmission and reception employed to minimize the effects of fading by the simultaneous use of two or more antennas spaced a number of wavelengths apart.

Space Operation Service—A radio communications service concerned exclusively with the operation of spacecraft, particularly space tracking, space telemetry, and space telecommand. These functions will normally be provided within the service in which the spacecraft is operating.

Space Radio Communications—Radio communications involving the use of one or more space stations, satellites, or other objects in space.

Space Station—A station located on an object which is beyond, is intended to go beyond, or has been beyond, the major portion of the earth's atmosphere.

Space Subsystem—In satellite communications, that portion of the satellite link that is in orbit.

Space System—All of the devices and organizations forming the space network. The network includes spacecraft, ground control stations, and associated terminals.

Space Telemetry—The use of telemetry for the transmission from a space station of results of measurements made in a spacecraft, including those relating to the functioning of spacecraft.

Spare Parts—Reparable components or assemblies used for maintenance replacement purposes in major end items of equipment.

Spares—(1) A generic maintenance and logistics term denoting both spare and repair parts, i.e., assemblies, sub-assemblies, or components used for the maintenance or repair of a (communications) system or equipment. (2) Recoverable items used in the repair of higher-level assemblies and which are themselves subject to repair on failure; recoverable items are not automatically discarded on failure.

Special Intelligence Communications (SPINTCOM)—A dedicated family of circuits, terminals, and facilities that serve the special security office functions at most major headquarters worldwide.

Specification—A document that prescribes, in a complete, precise, verifiable manner, the requirements, design behavior, or characteristics of a system or system component.

Spectrum Designation of Radio Frequencies—A method of referring to a range or band of radio frequencies. The following are the frequency designations and ranges:

Extremely Low Frequency (ELF):	below 30 Hz
Super Low Frequency (SLF):	30 to 300 Hz
Ultra Low Frequency (ULF):	300 to 3000 Hz
Very Low Frequency (VLF):	3 to 30 kHz
Low Frequency (LF):	30 to 300 kHz
Medium Frequency (MF):	300 to 3000 kHz
High Frequency (HF):	3 to 30 MHz
Very High Frequency (VHF):	30 to 300 MHz
Ultra High Frequency (UHF):	300 to 3000 MHz
Super High Frequency (SHF):	3 to 30 GHz
Extremely High Frequency (EHF):	30 to 300 GHz
Tremendously High Frequency (THF):	300 to 3000 GHz

Spectrum Management—Planning, coordinating, and managing joint use of the electromagnetic spectrum through operational, engineering, and administrative procedures, with the objective of enabling electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference.

Specular Reflector—Reflecting light in a diffuse manner.

Speech Synthesis—The generation of machine voice by arranging phonemes (for example, *k*, *ch*, *sh*, and so forth) into words. Speech synthesis performs real-time conversion without a predefined vocabulary, but does not create human-sounding speech. Although individual spoken words can be digitized into the computer, digitized voice takes a lot of storage, and the resulting phrases lack inflection.

Splice Loss—In optical fiber systems, any loss of optical power at a splice.

Splice Organizer—In optical fiber systems, a device that facilitates the splicing or breaking out of optical cable. The organizer provides means to separate and secure individual buffer tubes and, or fibers or pigtails. It also provides the means to secure mechanical splices or protective sleeves used in connection with fusion splices, and contain the slack fiber that remains after the splicing process is completed.

Split Knowledge—Separation of data or information into two or more parts, each part constantly kept under control of separate authorized individuals or teams, so that no one individual or team will know the whole data.

Spoofing—Attempt to gain access to a communications and information system by pretending to be an authorized user. Impersonating, masquerading, and mimicking are forms of spoofing.

Spread Spectrum System—A system that produces a signal with a bandwidth much wider than the intelligence or message bandwidth.

Spread Spectrum—(1) In general, a signal with a large time-bandwidth product. (2) A telecommunications technique in which the modulated information is transmitted in a bandwidth considerably greater than the frequency content of the original information. In satellite communications, spread spectrum may be employed as an anti-noise signal-gain processing tool.

Spurious Emission—In radio transmissions, an emission on frequencies that are outside the necessary bandwidth, the level of which may be reduced without affecting the corresponding transmission of information. Spurious emissions include harmonic emissions, parasitic emissions, intermodulation products, and frequency conversion products, but exclude out-of-band emissions.

Spurious Response—Any response of an electronic device to energy outside its designated reception bandwidth.

Stand-Alone—A system which performs its functions requiring little or no assistance from interfacing systems.

Standard Automated Logistics Tools Set—A client-server application used by Air Force post offices to transmit mail characteristics data to a central location from which the US Postal Service collects mail transit time information.

Standard Frequency and Time Signal Service—A radio communications service for scientific, technical, and other purposes, providing the transmission of specified frequencies and/or time signals of stated high precision intended for general reception.

Standard Publication—Doctrine documents, policy directives, instructions, mission directives, manuals, indexes, directories, handbooks, catalogs, operating instructions, supplements, pamphlets, visual aids, bulletins, and staff digests.

Standard Publication System—Standard publications announce policies, assign responsibilities, prescribe procedures, direct actions, and inform people

Standard Table—Column heads run across the page and the information in each column runs down the page.

Standardization—In the Department of Defense, the process by which the DoD achieves the closest practicable cooperation among its components; i.e., the most efficient use of research, development, and production rescues; agreement to adopt on the broadest possible basis the use of common or compatible operational, administrative, and logistics procedures and criteria; common or compatible technical procedures and criteria; common or compatible, or interchangeable supplies, components, weapons, or equipment; and common or compatible tactical doctrine with corresponding organizational compatibility.

Standardized General Markup Language (SGML)—Pertaining to electronic publishing, (1) an International Standards Organization (ISO) standard; a very powerful tool for creating electronic

documents with explicit organizing rules, i.e., the documents explain their own organization and content. It can be reused on various computer platforms and printed out; (2) The international standard metalanguage (a language for describing markup languages) that is used to facilitate the creation, management, storage, structure, and content of an electronic document.

Standardized Tactical Entry Point (STEP)—The STEP is a communications gateway that provides reachback into the Defense Information Systems Network (DISN) for deployed commanders. The STEP provides information (classified and unclassified) interchange, including voice, data, video, imagery, and message services (including the Automatic Digital Network and Defense Message System) from the deployed location via military satellite communications into the DISN.

Standards—An exact value, a physical entity, or an abstract concept established and defined by authority, custom, or common consent to serve as a reference, model, or rule in measuring quantities or qualities, establishing practices or procedures, or evaluating results. See Information Technology System (ITS) Standards.

Standards Profile—See Profile.

Start-Stop System—See Asynchronous System.

Start-Up Key-Encryption-Key (KEK)—Key-encryption-key held in common by a group of potential communicating entities and used to establish ad hoc tactical networks.

Station Battery—A separate battery power source within a communications facility that provides direct current power for all significant requirements associated with the facility.

Station Clock—A clock that controls some or all of the equipment in the station that require local time control.

Station Load—The total (alternating current) electrical power requirements of the integrated station facilities.

Statistical Multiplexing—Multiplexing in which channels are established on a statistical basis (i.e., connections are made according to probability of need).

Storage—(1) Maintaining information for later retrieval and access by the user. (2) Pertaining to a device into which data can be entered, held, and retrieved.

Store-and-Forward Message System—The communications process that allows messages to be stored at intermediate nodes before being forwarded to their destination.

Stovepipe System—A dedicated or proprietary system that operates independently of other systems. The stovepipe system often has unique, nonstandard characteristics.

Structured Protection (Class B2)—Enhanced-level trusted computing base that provides intermediate-level mandatory access control protection features, as well as enhanced DAC features. Sensitivity labels are used to enforce access control decisions and are based on a formally specified security policy model that documents rules for how each subject (users, programs) may access every object (files, records). Operational support features are provided, such as a Trusted Facility Manual, system security officer, and administrator functions, and stringent configuration management practices.

Structured Query Language (SQL)—A database language. It is a unified language that allows data definition, manipulation, and control. The language was developed to access relational databases.

Subcarrier—In frequency division multiplexing, a carrier used to modulate another carrier. The resultant

modulated carrier can be used to modulate another carrier, and so on, so that there can be several levels of subcarriers or intermediate carriers.

Subject Security Level—Sensitivity labels of the objects to which the subject has both read and write access. Security level of a subject must always be dominated by the clearance level of the user associated with the subject.

Sublayer—In a layered open communications system, a specified subset of the services, functions, and protocols included in a given layer.

Subnetwork—A collection of equipment and physical transmission media that forms an autonomous whole and that can be used to interconnect systems for the purposes of communication.

Subroutine—A sequence of instructions that tell the computer to perform a specific task. This sequence of instructions is usually considered as a separate routine. It may also be a part of a larger routine that can be compiled separately, but usually cannot be run as a separate program.

Subscriber—In a public telecommunications network, the ultimate user, i.e., the customer, of a communications service. Subscribers include individuals, activities, organizations, etc. Subscribers use end instruments, such as telephones, modems, facsimile, computers, and remote terminals. Subscribers do not include communications systems operating personnel, except for their personal terminals.

Subsystem—(1) A functional grouping of components that combine to perform a major function within a system. (2) A major functional subassembly or grouping of items which is essential to the operational completeness of a system.

Super Synchronous Orbit (SSO)—A final orbit location to which satellites are sent that are no longer operationally functional.

Superencryption—Process of encrypting encrypted information. Occurs when a message, encrypted off-line, is transmitted over a secured, on-line circuit, or when information encrypted by the originator is multiplexed onto a communications trunk, which is then bulk encrypted.

Supersession—Scheduled or unscheduled replacement of a COMSEC aid with a different edition.

Superuser—Special user who can perform control of processes, devices, networks, and file systems.

Supervisory Signals—Signals used to indicate and/or control the various operating states of the circuits and/or equipment assemblies of a communications system.

Supply Support—All management actions, procedures, and techniques necessary to acquire, catalog, receive, store, transfer, issue, and dispose of secondary items. It includes provisioning for initial support, as well as acquiring, distributing, and replenishing inventory spares and parts, and planning for

Support Equipment (SE)—In logistics, all equipment (mobile and/or fixed) required to support the operation and maintenance of a weapon system, except that which is an integral part of the mission equipment. Trainers and simulators are not support equipment.

Support Item—In logistics, a term indicating spares, repair parts, equipment items, or equipment items.

Supportability—The degree of ease to which system design characteristics and planned logistics resources, including logistics support elements, allows for the meeting of system availability and wartime utilization requirements.

Surface Wave—In radio communications, a radio frequency wave that propagates close to the surface of

the earth. Synonym: Ground wave.

Surveillance Television (STV)—A closed-circuit television system that provides a visual representation of secure and hazardous areas for remote monitoring.

Survivability—Capability of a system to accomplish its mission in the face of an unnatural (man-made) hostile, scenario-dependent environment. Survivability may be achieved by avoidance, hardness, proliferation, reconstitution or a combination thereof.

Susceptibility—(1) The degree to which a device, equipment, or system is open to effective attack due to one or more inherent weaknesses. Susceptibility is a function of operational tactics, enemy countermeasures, etc. Susceptibility is considered a subset of survivability. (2) Inability of a system to prevent: (a) an electronic compromise of national security information or, (b) detrimental effects on its operational integrity.

Switched Multi-megabit Data Service (SMDS)—A high speed (1.544 Mbps to 45 Mbps), connectionless, packet-switched service allowing local area network-like performance and features over a metropolitan or wide area network. SMDS is not a protocol, but rather a service that operates independently of the underlying protocol. SMDS is a stepping stone to asynchronous transfer mode (ATM) because of its forward compatibility with ATM and compatibility with frame relay.

Syllabary—List of individual letters, combination of letters, or syllables, with their equivalent code groups, used for spelling out words or proper names not present in the vocabulary of a code. A syllabary may also be a spelling table.

Symbolic Language—A computer programming language used to express addresses and instructions with symbols convenient to humans rather than to machines.

Synchronous—In communications-electronics, pertaining to the relationship of two or more repetitive signals that have simultaneous occurrences of significant instants.

Synchronous Crypto-Operation—Method of on-line crypto-operation in which cryptoequipment and associated terminals have timing systems to keep them in step.

Synchronous Optical Network (SONET)—A set of specifications and concepts for high speed optical transport over fiber multiplexed systems. It has the distinct advantage of providing (a) a standardized optical interface and signaling format across all fiber systems, (b) advanced maintenance and network management features, and (c) easier add-drop multiplexing for network inter-connections and rearrangements. SONET deployment can increase network survivability.

Synchronous Orbit—An orbit in which a satellite has a velocity synchronized to the speed of the rotation of the earth and thus remains above a fixed point on the earth's surface. This occurs at an altitude of approximately 22,300 miles over the equator and the gravitational pull of the earth equals the centrifugal force acting upon the satellite.

Synchronous Satellite—A satellite in a synchronous earth's orbit.

Synchronous System—In communications-electronics, a system in which events such as signals occur in synchronism. A system in which the transmitter and receiver functions are operating in a fixed time relationship.

Synchronous Transmission—1. A form of data transmission in which transmitting and receiving stations are synchronously timed to eliminate the need for stop-and-start bits. 2. A transmission process

such that between any two significant instants in the overall bit stream, there is always an integral number of unit intervals. Compare with Asynchronous Transmission.

Syntonization—In communications-electronics, the process of setting the frequency of one oscillator equal to that of another.

System—1. Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. 2. The organization of hardware, software, materiel, facilities, personnel, data, and services needed to perform a designated function with specified results, such as the gathering of data, its processing, and delivery to its users. 3. A combination of two or more interrelated pieces of equipment (sets) arranged in a functional package to perform an operational function or satisfy a requirement.

System Administrator (SA)—Individual responsible for the installation and maintenance of an Information System, providing effective information system utilization, adequate security parameters, and sound implementation of established information systems security policy and procedures.

System Control—In satellite communications, system control of communications satellites embodies several different control functions that are accomplished by different levels or types of commands and which may be done by the same or separate control facilities. Control functions relate to: (a) Operational Control. The control exercised to determine the location of satellites, the location of fixed earth terminals, and the parameters required for operation of the earth segment, such as allocation of satellite power, bandwidth, access time, and operating frequencies (channels); (b) Satellite Communication Control. The control of a satellite exercised by a master station to ensure that the earth segment operates within its assigned parameters and according to prescribed procedures; (c) Satellite Control. The manipulative control and monitoring of onboard subsystems and components of a satellite, including those affecting position and attitude as well as the adjustment and switching of subsystems or components.

System Development Methodologies—Methodologies developed through software engineering to manage the complexity of system development. Development methodologies include software engineering aids and high-level design analysis tools.

System Engineering—A comprehensive, iterative technical management process that includes translating operational requirements into configured systems, integrating technical data, managing interfaces, characterizing and managing technical risk, transitioning technology from the technology base into program specific efforts, and verifying that designs meet operational needs.

System High Mode—Information system security mode of operation wherein each user, with direct or indirect access to the Information System, its peripherals, remote terminals, or remote hosts, has all of the following: (a) Valid security clearance for all information within an Information System. (b) Formal access approval and signed non-disclosure agreements for all the information stored and/or processed (including all compartments, subcompartments and/or special access programs). (c) Valid need-to-know for some of the information contained within the information system.

System Integrity—1. Quality of an information system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. 2. The attribute of a system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

System Profile—Detailed security description of the physical structure, equipment component, location, relationships, and general operating environment of an information system.

System Security Authorization Agreement (SSAA)—Applicable set of planning and certification actions, resources, and documentation required to support the certification and accreditation. It guides the implementation of information protection requirements and the resulting certification and accreditation actions.

System Security Engineering—The effort to achieve and maintain optimal security and survivability of a system throughout its life cycle.

System Security Management Plan—Formal document fully describing the responsibilities for security tasks planned to meet system security requirements.

System Security Plan—Formal document fully describing the planned security tasks required to meet system security requirements.

System Security Policy—Set of laws, rules, and practices that regulate how sensitive (SBU and classified) information is managed, protected, and distributed by an AIS. NOTE**:** System security policy interprets regulatory and operational requirements for a particular system and states how that system will satisfy those requirements. All systems or networks that process SBU or classified information, will have a security policy.

Systems Architecture—The systems architecture shows how multiple systems within a subject area link and interoperate, and may describe the internal construction or operations of particular systems within the architecture. It is constructed to satisfy operational architecture requirements per standards defined in the technical architecture. It defines the physical connection, location, and identification of key nodes, circuits, networks, warfighting platforms, etc. and specifies system and component performance parameters.

Systems Control—In telecommunications, a set of processes, procedures, hardware, automated data processing equipment, communications, and personnel to perform a specific set of subfunctions that consist of facility surveillance, traffic surveillance, network control, traffic control, and technical control.

Systems Engineering—A comprehensive, iterative, technical management process that includes translating operational requirements into configured systems, integrating the technical inputs of the entire design team, managing interfaces, characterizing and managing technical risks, transistioning technology from the technology base into program specific efforts, and verifying that designs meet operational needs. It is a life cycle activity that demands a concurrent approach to both product and process development.

Systems Telecommunications Engineering Manager (STEM)—A C4 systems engineer who provides technical engineering planning services in support of C4 systems and base infrastructures. The base-level STEM (STEM-B) has technical responsibility for engineering management and assists the base communications and information systems officer in system engineering and configuration control. The command-level STEM (STEM-C) provides technical assistance to the major commands (MAJCOM) and coordinates with STEM-Bs on future MAJCOM mission changes, programs, and efforts at the MAJCOM level.

Tag Image File Format (TIFF)—In computer graphics, a file format for storing an image using the particular data structure of the file.

Talking Battery—In telephony, the dc voltage supplied by the central office to the subscriber's loop to operate the transmitter in the handset.

Tandem—1. The connection of the output terminals of one network, circuit, or link, directly to the input

terminals of another network, circuit, or link (for example, a microwave radio relay system employs tandem links). 2. A telecommunications switching arrangement whereby the trunk from a calling switch is connected to the trunks of a called switch through one or more intermediate switches which are referred to as "tandem switches" or "network tandems."

Target Architecture—The definition of the architecture components and their key attributes needed to support an organization over an agreed-upon planning interval (usually 3-5 years). It must be consistent with the organization's long-term objectives.

Tariff—Rates or charges for a business or public utility by commercial telephone companies and filed with a public regulatory agency.

T-Carrier System—A digital data carrier system that may be submultiplexed in many different ways to provide both analog and digital data services. (If the T is preceded by an F, fiber optic cable system is indicated using the same rates). T-carrier systems were originally designed to transmit digitized voice signals; current applications also include digital data transmissions. The designators for T-carrier in the North American digital hierarchy correspond to the designators for the digital signal (DS) level hierarchy.

Technical Architecture—1. The technical architecture identifies the services, interfaces, standards, and their relationships. It provides the technical guidelines for the implementation of systems upon which engineering specifications are based, common building blocks are built, and product lines are developed. *(DoD)* 2. A minimal set of rules governing the arrangement, interaction and interdependence of system parts or elements whose purpose is to ensure that a conformant system satisfies a specified set of requirements.

Technical Attack—An attack that can be perpetrated by circumventing or nullifying hardware or software protection mechanisms, or exploiting hardware or software vulnerabilities, rather than physical destruction or by subverting system personnel or other users.

Technical Control Facility (TCF)—A physical plant, or a designated and specially configured part thereof, containing the necessary distribution frames and associated panels, jacks, and switches; monitoring, test, and conditioning equipment; and orderwire/service channel communications to enable technical control personnel to exercise essential operational control over communications systems. Technical control includes the real-time transmission system configuration control, quality assurance, quality control, alternate routing, patching, testing, directing, coordinating, restoring, and reporting functions necessary for effective maintenance of transmission paths and facilities.

Technical Data—Recorded information regardless of form and of a technical nature, to include software documentation, that relates to supplies approved for procurement.

Technical Data Package (TDP)—A technical description of an item adequate for supporting an acquisition strategy, production, engineering, and logistics support. The description defines the required design configuration and procedures to ensure adequacy of item performance. It consists of all applicable technical data, such as drawings, associated lists, specifications, standards, performance requirements, quality assurance provisions, and packaging details.

Technical Information—Information, including scientific information, that relates to research, development, engineering, test, evaluation, production, operation, use, and maintenance of munitions and other military supplies and equipment.

Technical Interface—The functional, electrical, and physical characteristics necessary to allow the exchange of information across an interface between different C4(I) systems or equipment. Includes

Technical Interface Standards.

Technical Interface Standards—Specifications for functional, electrical, and physical characteristics necessary for exchanging information across an interface between different tactical C4I systems or equipment.

Technical Load—The portion of the operational (electrical) load required for communications, tactical operations, and ancillary equipment including necessary lighting, air conditioning, or ventilation required for full continuity of communications.

Technical Manual (TM)—A publication that contains instructions for the installation, operation, maintenance, training, and support of weapon systems, weapon system components, and support equipment. Technical Manual information may be presented in any form or characteristic, including, but not limited to hard copy, audio and visual displays, magnetic tape, disks, and other electronic devices. A Technical Manual normally includes operational and maintenance instructions, parts lists or parts breakdown, and related technical information or procedures exclusive of administrative procedures. Technical orders that meet the criteria of this definition may also be classified as technical manuals.

Technical Order (TO)—Publications of a technical nature which provide technical instructions to install, operate, maintain, and modify systems and equipment.

Technical Reference Codes (TRC)—A compendium of interoperability references (policy, directives, transition guidance, and standards). TRCs have been developed for planning, acquiring, and implementing interoperable, scalable, and portable Air Force information technology systems, system components, and services.

Technical Reference Model (TRM)—A common vocabulary and set of services and interfaces common to DoD information systems. The associated standards profile identifies standards and guidelines in terms of the reference model services and interfaces. These standards and guidelines can be applied and tailored to meet specific mission area requirements.

Technical Solution—A detailed description of the hardware, software, data, connectivity, logistics support, and other resources necessary to provide the most cost-effective solution to correct a deficiency or shortfall in mission capability. It includes the recommended acquisition method and strategy, estimates of all one-time and recurring costs, identification of manpower requirements (additional or savings estimate), and a schedule of events.

Technical Vulnerability—Hardware, firmware or software flaw that leaves a communications and information system open for potential exploitation. The exploitation can be either from an external or internal source, there by resulting in risk for the owner, user, or manager of the system. Note: The vulnerability must be demonstrable and repeatable, and validated by either the Air Force Information Warfare Center (AFIWC) or a national agency with validation authority.

Telecommunications—1. Any transmission, emission, or reception of signs, signals, writings, images, and sounds or information of any nature by wire, radio, visual, or other electromagnetic systems from one user to another. 2. Transmitting, communicating, or processing information, including preparing such information by electrical, electromagnetic, electromechanical, or electro-optical means.

Telecommunications Infrastructure—The organizations, personnel, procedures, facilities, and networks employed to transmit and receive information by electrical or electronic means. Telecommunications facilities include, but are not limited to, terrestrial radio, metallic and optical fiber cables, artificial earth satellite communications, radio and television stations (traditional broadcast as well

as cable and satellite broadcast), public switched telephone networks, etc. Examples of advanced telecommunications infrastructure facilities are direct broadcasting, digital television, and the global positioning system (GPS).

Telecommunications Security—See Information Systems Security.

Telecommunications Service Order (TSO)—The authorizing and specifying order from the Defense Information Systems Agency to start, change, or discontinue circuits or trunks, or to effect administrative changes.

Telecommunications Service Request (TSR)—A validated message request for service that details the type of service, service locations, and other pertinent information required to specify parameters to the agency or commercial carrier providing the service.

Telecommunications System Standards (TCSS)—A standardization area of the Defense Standardization Program. This area establishes uniform engineering criteria for terminal equipment, transmission equipment and media, and switching equipment in military telecommunications interoperability with non-military systems that support military functions. Activities within the TCSS area include participating in Federal, commercial, and international standardization efforts as well as developing military unique telecommunications standards.

Teleconference—A conference between persons remote from one another but linked by a telecommunications system.

Telegraphy—A form of telecommunication for the transmission of written matter by the use of a signal code, such as the Morse code.

Telemetry—The use of telecommunications for the transmission of information on measurements. The outputs from instruments or sensors are carried, usually via line-of-sight microwave radio links, to a station or facility where the signals can be observed, recorded, and/or analyzed. The instruments or sensors can be located on a stationary or moving platform.

Teleport—In satellite communications, a ground station that provides an interface to the Global Grid, cross-banding between satellites operating at different frequencies, and a gateway function between satellite operating at the same frequency.

Teleprocessing—1. Data processing using computers and communications facilities. 2. A combination of telecommunications and computer operations that interact in the automatic processing, reception, and transmission of data or information.

Telnet—The Internet standard protocol to connect to remote terminals.

TEMPEST Zone—Designated area within a facility where equipment with appropriate TEMPEST characteristics (TEMPEST zone assignment) may be operated.

TEMPEST—1. Short name referring to investigation, study, and control of compromising emanations from information systems equipment. 2. An unclassified term referring to technical investigations for compromising emanations from electrically operated information processing equipment; these investigations are conducted in support of emanations and emissions security.

TEMPEST-Certified Equipment—Systems or equipment which were certified within the requirements of the effective edition of NSTISSAM TEMPEST/1-92, Level I, or TEMPEST specifications as determined by the department or agency concerned.

Template—1. A document that describes a customer's operational architecture (information flow) and provides an as-is (baseline) and to-be systems architecture using DoD, Air Force, and other applicable technical architectures in the recommended solutions. A template ties operational, system, and technical architectures together for the customer based on the customer's specified area of interest (that is, a specific system, process, and, or facility). The template is customer focused. 2. A form displayed on a computer monitor into which you enter data for processing.

Tera (T)—A prefix used to denote trillion (10^{12}).

Terahertz (THz)—A unit denoting one trillion hertz.

Terminal Equipment—Communications equipment at each end of a circuit or channel to permit the stations involved to accomplish the purpose for which the circuit or channel was established.

Test Form—A form established to be used for a limited period of time so it may be evaluated by testing activities. If not converted to a permanent form by the expiration date, it automatically becomes obsolete.

Test Tone—In telecommunications, a single-frequency sinusoidal signal used by maintenance or technical controller personnel to test, troubleshoot or align communications circuits or components. In earlier analog systems, typically an (audible) 1 kHz frequency was used, hence the term test tone. Also called a tone, for short. May refer to the use of a signal of any frequency for testing purposes.

Thermal Noise—In communications-electronics. Random, undesirable electrical signals generated by thermal agitation of electrons in a conductor.

Thin Client—A computer limited to only the essential applications and capabilities. A low-cost, centrally managed computer devoid of CD-ROM player, diskette drive, expansion slots, etc.

Threat/Vulnerability Assessment—An observation of the vulnerabilities, threats, likelihood, loss or impact, and theoretical effectiveness of security measures. Managers use the results to develop security requirements and specifications (what do I have versus what do I want).

Threat—1. Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. 2. Current and perceived capability, intention, or attack directed to cause denial of service, corruption, compromise, or fraud, waste, and abuse to a system.

Ticket-Oriented—In communications security, a computer protection system in which each subject maintains a list of unforgeable bit patterns called tickets, one for each object that a subject is authorized to access. See List-Oriented.

Tie-Line Service—Direct trunks between two telephone exchanges that have dial-to-dial termination. When a base or activity needs frequent telephone contact with another government agency or customer served by a different telephone exchange, direct tie-lines are usually more economical and convenient.

Time Division Multiple Access (TDMA)—In satellite communications, the use of time interlacing to provide multiple and apparently simultaneous access to a single transponder with a minimum of interference.

Time Division Multiplexing (TDM)—The process or device in which each modulating wave modulates a separate pulse subcarrier, the pulse subcarriers being spaced in time so that no two pulses occupy the same transmission interval. Time division permits the transmission of two or more signals over a common path by using different time intervals for the transmission of the intelligence of each message signal.

Timing Signal—1. The output of a clock. 2. A signal used to synchronize interconnected equipment.

Toll Quality—In telephony, the high correlation between the intelligibility and quality of electronically transmitted voice with that of the natural human voice.

Tone—See Test Tone.

Top-Level Specification—Nonprocedural description of system behavior at the most abstract level; typically, a functional specification that omits all implementation details.

Topology—The layout of nodes (switches, concentrators) and transmission paths of a network.

Touch Interactive Display (TID)—Uses a physical device between the user and the display that acts as the input mechanism.

Traditional Communications Security Program—Program in which the National Security Agency acts as the central procurement agency for the development and, in some cases, the production of information systems security items. This includes the Authorized Vendor Program. Modifications to the Information Systems Security end items used in products developed and/or produced under these programs must be approved by the National Security Agency.

Traffic—The information moved over a communications channel. A quantitative measurement of the total messages and their length, expressed in hundred-character seconds (cluster control units) or other units, during a specified period of time.

Traffic Encryption Key—Key used to encrypt plain text or to superencrypt previously encrypted text and/or to decrypt cipher text.

Traffic Padding—Generation of spurious communications or data units to disguise the amount of real data units being sent.

Traffic-Flow Security—Measure used to conceal the presence of valid messages in an on-line cryptosystem or secure communications system.

Training Key—Cryptographic key for training.

Transaction Set—In electronic data interchange, the data sent by one trading partner to another that allows recipient to complete a single transaction, essentially a complete business document.

Transceiver—Combination of transmitter and receiver. An item of equipment, device, or circuit that can both transmit and receive signals (for example, telephone, two-way radio). This term is sometimes also applied to a terminal with facilities for both sending and receiving messages.

Transient—An unpredictable short-duration change in circuit condition; a pulse or increase in circuit noise. An example is impulse noise in a communications circuit.

Transliteration—1. Code conversion; a change of the bit patterns used to represent the characters of a set. 2. A change in the representation of characters. 3. An erroneous substitution of one bit or character for another.

Transmission—1. The dispatching, for reception elsewhere, of a signal, message, or other form of information. 2. The propagation of a signal, message, or other form of information by any medium such as wire, coaxial cable, optical fiber, or radio wave.

Transmission Facility—In telecommunications, a cable, radio, or satellite communications facility that provides a transmission medium for the Defense Switched Network (DSN) interswitch trunks and access

lines.

Transmission Security (TRANSEC)—A component of communications security resulting from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.

Transmission Security Key—A key used in the control of TRANSEC processes, such as frequency hopping and spread spectrum.

Transmit Clock—The clock (timing signal source) from which the transmitting circuitry of a modem obtains its timing.

Trap Door—Hidden software or hardware mechanism used to circumvent security controls.

Tremendously High Frequency (THF)—Frequencies of electromagnetic waves in the range of 300 to 3000 gigahertz.

Tri-axial Cable—A specialized form of coaxial cable, circular in cross-section and consisting of (a) a center conductor, often a solid wire but sometimes braided; separated by an insulating material from (b) a concentric solid or braided conductor which is in turn separated by an insulating material from (c) a third solid or braided conductor, concentric with the first two; and (d) a protective sheath. In a tri-axial cable, the third conductor can act as a shield, being grounded at one end and not connected at the other.

Tributary Station—Also slave station, secondary station, or data station. In a data network, a station other than the master station.

Trojan Horse—Program containing hidden code allowing the unauthorized collection, falsification, or destruction of information.

Tropospheric Scatter Communications—A type of wideband radio communications that uses the troposphere to scatter and reflect the radio waves, thus providing communications between stations that are not in line-of-sight. Tropospheric scatter links operate in the ultra high frequency range for distances up to 600 miles. Once a popular long-haul communications method, most fixed tropospheric scatter links have been replaced by satellite communications.

Truncate—To remove leading or trailing digits from a number without regard to the effect on the remaining digits.

Trunk Exchange—The elements of a telephone exchange that perform the interconnection of trunks.

Trunk—1. A single transmission channel between two points, both of which are switching centers or nodes, or both. 2. In a telephone system, a multiple circuit connection between two exchanges. 3. A communications channel between two different offices or between groups of equipment within the same office.

Trunking—In land mobile radio (LMR), trunking is defined as the automatic time-sharing of a small number of frequency resources (channels) to serve a large number of users. The relatively short duration of an individual LMR call can allow channels of a trunked LMR system to be shared in a very spectrum-efficient manner. Trunking systems offer more flexibility than conventional non-trunked systems.

Trusted Computer System—1. A data processing system that provides sufficient computer security to allow for concurrent access to data by users with different access rights and to data with different security classification and security categories. 2. Information system that employs sufficient hardware and

software assurance measures to allow simultaneous processing of a range of classified or sensitive information.

Trusted Computer System Evaluation Criteria (TCSEC) Nomenclature—System for identifying the type and purpose of certain items of communications security material.

Trusted Computing Base (TCB)—The totality of protection mechanisms within a computer system--including hardware, firmware, and software--the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a TCB to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy.

Trusted Distribution—Method for distributing trusted computing base hardware, software, and firmware components that protects the trusted computing base from modification during distribution.

Trusted Facility Management—Administrative procedures, roles, functions, privileges, and databases used for secure system configuration, administration, and operation.

Trusted Facility Manual—Document containing the operational requirements; security environment; hardware and software configurations and interfaces; and all security procedures, measures, and contingency plans.

Trusted Identification Forwarding—Identification method used in information system networks whereby the sending host can verify that an authorized user on its system is attempting a connection to another host. The sending host transmits the required user authentication information to the receiving host.

Trusted Network—Network that employs sufficient hardware and software integrity measures to allow its use for processing simultaneously a range of sensitive or classified information.

Trusted Path—Mechanism by which a person using a terminal can communicate directly with the trusted computing base (TCB). Trusted path can only be activated by the person or the TCB and cannot be imitated by untrusted software.

Trusted Process—Process that has privileges to circumvent the system security policy and has been tested and verified to operate only as intended.

Trusted Recovery—Ability to ensure recovery without compromise after a system failure.

Trusted Software—Software portion of a trusted computing base.

Twisted Pair—A pair of individually insulated conductors (wires) twisted together and treated as an entity in the transmission of electrical signals or power. In communications cables, the twisted pair is typically composed of two individually insulated solid copper wires. Because the wires are twisted together, interfering signals tend to create opposing electromagnetic forces at frequent intervals, reducing the effect of the interference on the signal(s) being conducted. Twisted pairs may be used for bit rates up to 1 Mb/s over short distances (<100 m) and lower bit rates over longer distances.

Two-Person Control—Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements.

Two-Person Integrity (TPI)—System of storage and handling designed to prohibit individual access to certain communications security keying material by requiring the presence of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed. See No-Lone Zone.

Two-Wire Circuit—In telecommunications, a full-duplex communications circuit that utilizes only two metallic conductors, e.g., a single twisted pair.

Type 1 Encryption Product—Classified or controlled cryptographic item endorsed by the National Security Agency for securing classified and sensitive U.S. Government information, when appropriately keyed. Type I products contain classified National Security Agency algorithms.

Type 1 Product—Classified or controlled cryptographic item endorsed by the National Security Agency for securing classified and sensitive U.S. Government information, when appropriately keyed. The term refers only to products, and not to information, key, services, or controls. Type 1 products contain classified National Security Agency algorithms. They are available to U.S. Government users, their contractors, and federally sponsored non-U.S. Government activities subject to export restrictions in accordance with International Traffic in Arms Regulation.

Type 2 Product—Unclassified cryptographic equipment, assembly, or component, endorsed by the National Security Agency , for use in an information system for the protection of sensitive unclassified information identified as Warner Amendment (Title 10 U.S.C. Section 2315).

Type 3 Algorithm—Cryptographic algorithm registered by the National Institute of Standards and Technology (NIST) and published as a Federal Information Processing Standard (FIPS) for use in protecting unclassified sensitive information or commercial information.

Type 4 Algorithm—Unclassified cryptographic algorithm that has been registered by the National Institute of Standards and Technology (NIST), but not published as a Federal Information Processing Standard (FIPS).

Type Accreditation—1. Designated approving authority authorization to employ a number of systems in a specified operational environment. To be type accredited, the systems must have similar characteristics, such as same function, physical environment, operating system, security subsystem, and so on. See **Accreditation**2. The official authorization by the accreditor to employ a system in a specified environment. It includes a statement of residual risk, delineates the operating environment, and identifies specific use, operational constraints, and/or procedural work around. It may be performed when multiple platforms will be fielded in similar environments.

Type Designation—A specific combination of letters and numerals, structured in accordance with Military-Standard (MIL-STD) 196, *Joint Electronic Type Designator (JETD) System*, that provides a standard means of uniquely identifying electronic equipment by design configuration (for example, AN/TRC-97).

Type II Encryption Product—Unclassified cryptographic equipment, assembly, or component, endorsed by the National Security Agency, for use in telecommunications and automated information systems for the protection of national security information. Type II products may not be used for classified information, but contain classified National Security Agency algorithms that distinguish them from products containing the unclassified data encryption standard algorithm.

Ultra High Frequency (UHF)—Frequencies of electromagnetic waves in the range from 300-3000 megahertz.

Ultra Low Frequency (ULF)—Frequencies of electromagnetic waves in the range from 300-3000 hertz.

Unauthorized Disclosure—Exposure of information to individuals not authorized to receive it.

Unbalanced Line—In telecommunications, a transmission line in which the magnitudes of the voltages on the two conductors are not equal in respect to ground (for example, a coaxial line).

Unclassified—Information that has not been determined pursuant to Executive Order 12958 or any predecessor order to require protection against unauthorized disclosure and that is not designated as classified.

Unified Mail—The ability to store messages of all types (voice, fax, email, video, paging, etc.) in one mailbox with accessibility from either a PC or telephone.

Unified Messaging—The ability to create and respond to multimedia messages from either a PC or telephone (especially across different vendor platforms)

Uniform Resource Identifier (UFI)—A general name that can refer to either a Uniform Resource Locator (URL) or Uniform Resource Name (URN). It is used when it is unclear or does not matter whether the referenced item is a URL or URN.

Uniform Resource Locator (URL)—An Internet "address" of a resource; a pointer to a specific address on the web. On the World Wide Web, URLs represent hypermedia links and links to network services within Hypertext Markup Language documents. A URL can represent nearly any file or service on the Internet. The first part of the URL specifies the method of access; the second is typically the address of the computer where the data or service is located; further parts may specify names of files, port to which to connect, or the text to search for in a database.

Uniform Resource Name (URN)—In web site addressing, a URN uniquely identifies an entity, but not its location. This arrangement allows the system to check if a local copy exists, before going to find it on the web. It also allows a web locations to change, while still allowing the object to be found.

Unintelligible Crosstalk—Crosstalk given rise to unintelligible sounds.

Uninterruptible Power Supply (UPS)—In computing, a device inserted between a power source and a system to ensure that the system is guaranteed a precise, uninterrupted power supply, irrespective of variations in the power source voltage.

Unipolar—In data communications, pertaining to a signal that has excursions from zero to either a positive or negative value, but not both. (e.g., consists of a stream of positive pulses only).

Universal Messaging—The ability to create any type of message and to send it to anyone without regard to the recipient's mailbox requirements

Unofficial Commercial Service—Telephone service that directly connects private telephones to a commercial telephone exchange. Not required for conduct of official business. This includes telephone service in military housing, non-appropriated fund facilities, commercial activities, and other facilities.

Unscheduled Maintenance—Also referred to as Corrective Maintenance, includes all maintenance actions to restore an item of equipment or system to a specified condition as a result of a failure.

Unscheduled Record—A record whose disposition is waiting on the National Archives and Records Administration's final approval.

Untrusted Process—In Information Assurance, a process that has not been evaluated or examined for

adherence to the security policy. It may include incorrect or malicious code that attempts to circumvent the security mechanisms.

Uplink—In satellite communications, that portion of a communications link from the earth terminal to the satellite.

User—1. A person or organizational unit responsible for applying an automated or manual procedure to support the execution of a process. 2. Any person, organization, or functional unit that uses the services of an information processing system.

User Datagram Protocol (UDP)—In networking, a communications protocol offering a limited amount of service when exchanging messages on a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP), and together with IP, is sometimes referred to as UDP/IP. Like the TCP, UDP uses the IP to actually get a data unit (called a datagram) from one computer to another.

User Friendly—Designating a computer, terminal, program, and so forth, that is easily used and understood by a wide variety of people.

User Interface—In man-machine interfaces, the interface through which the user and a system or computer communicate. It includes input and output devices, such as a keyboard, printer, and display, and also the software-controlled means by which the users are prompted to supply data needed by the application, and by which they are notified of their errors and how to correct them.

User Profile—1. In computer networking, a description of an authorized user, typically for the purpose of access control. A user profile may include data such as user ID, user name, password, access rights, and other attributes. 2. A pattern of a user's activity that can be used to detect changes in the activity.

Utility Program—A computer program designed to perform common routine tasks (for example, copying files).

Valid Password—Personal password that authenticates the identity of an individual when presented to a password system or an access password that allows the requested access when presented to a password system.

Validation—Process of applying specialized security test and evaluation procedures, tools, and equipment needed to establish acceptance for joint usage of an information system by one or more departments or agencies and their contractors.

Variable Costs—Costs that rise and fall as production increases and decreases. Such costs include supplies, contract maintenance agreements, and some rentals. The manager should use care in cutting expenses in these areas, as it could drive costs up in other areas. For example, savings from bulk purchases of paper supplies can increase warehouse costs, and personnel costs to manage the stock. Buying inexpensive supplies that turn out to be of inferior quality can create equipment operating problems, reducing personnel productivity and increasing the total cost of production.

Verification—Process of comparing two levels of an information system specification for proper correspondence (e.g., security policy model with top-level specification, top-level specification with source code, or source code with object code).

Verified Design—Computer protection class in which formal security verification methods are used to assure that mandatory and discretionary security controls can effectively protect classified and sensitive information stored in, or processed by, the system. Class A1 system is verified design.

Very Low Frequency (VLF)—Frequencies of electromagnetic waves in the range of 3-30 kilohertz.

Vestigial Sideband (VSB) Transmission—In radio communications, a modified amplitude modulation transmission in which one sideband, the carrier, and only a portion of the other sideband are transmitted.

Video Random Access Memory (VRAM)—Random access memory that is used to hold data that defines an image displayed on the monitor.

Video Teleconferencing (VTC)—A telecommunications system that encompasses video, data, and voice components. VTC is a real-time electronic means of communicating visual, audio, and graphics information from one location to another, or among multiple locations. VTC may also include teletraining or distance learning to provide interactive remote site training.

Virtual—A term used in various ways to indicate that the actual physical implementation (storage, peripheral device, communications circuit) is different from that perceived by a user or user program.

Virtual Disk—In memory systems, an area of main storage in which the data is structured as if it were stored on a floppy disk.

Virtual Memory—In computer memory systems, this term describes memory or a computer storage location that is used to simulate another type of memory or storage even though it does not physically exist. It is a technique that allows the processor to employ its full address space although it exceeds the physical main memory available. The virtual memory space exists on the disk, when the processor addresses a portion of its address space outside the main memory, special hardware locates the required page on the disk and transfers it to a section of the main memory.

Virtual Network—A network that provides virtual circuits and that is established by using the facilities of a real network.

Virtual Office—A work environment where employees work cooperatively away from the central work place, typically at their homes, using a computer network

Virtual Private Network (VPN)—A logical data network configuration that makes use of a public or common user telecommunications infrastructure to simulate a private data network providing integrity, authentication, and confidential cryptographic services for network applications. The enterprise objective of a VPN is to provide secure network services at lower cost by optimizing the common public infrastructure.

Virtual Reality (VR)—Computer-generated images and sounds representing real-world environments. VR is an interactive technology that creates the illusion that one is immersed in a world created by the computer (program). It is fundamentally a communications medium that transforms information from a computer to a person through the senses. VR systems place the user in an artificial environment that the user can manipulate.

Virtual Reality Modeling Language—A draft specification for the design and implementation of a platform independent language for virtual reality scene description.

Virtual Terminal—The ability for terminal systems and host applications on a network to communicate without requiring either side to know the terminal characteristics of the other; provides an implementation-independent and interoperable teletype function capable of a simple character/lines dialog, and also a forms capability intended to support forms-based applications with local entry. It can speed up the operation of microcomputer software that is designed to extract its data from a floppy disk.

Visual Information (VI)—Use of one or more of the various visual media with or without sound. Generally, VI includes still photography, motion picture photography, video or audio recording, graphic arts, visual aids, models, display, visual presentation services, and the supporting processes.

Visual Information (VI) Documentation (VIDOC)—Motion media, still photography, and audio recording of technical and nontechnical events, as they occur, usually not controlled by the recording crew.

Visual Information (VI) Products—VI media elements such as still photography (photographs, transparencies, slides, and filmstrips), audio and video recordings (tape or disk), graphic arts (including computer-generated products), models, and exhibits. VI production is a unique form of VI product and usually is addressed separately.

Visual Information (VI) Systems—Visual information systems include still and motion picture photography, video and audio recording, video teleconferencing, graphic arts, base government-access channel television, visual aids and displays, visual presentation services, and supporting processes.

Visual Information Support Center (VISC)—Visual Information (VI) activities that provide general support to all installation, base, facility, or site organizations or activities. Typically, VISCs provide laboratory support, graphic arts, VI libraries, and presentation services.

Vital Records—Records essential to the continued functioning or reconstitution of an organization during and after an emergency and also those records essential to protecting the rights and interests of that organization and of the individuals directly affected by its activities.

Voice Frequency (VF) Channel—A transmission path or channel, normally part of a communications system, suitable for carrying analog signals and quasi-analog signals under certain conditions. In DoD communications systems, a VF channel accommodates input signals in the range of 300-3400 hertz.

Voice-over-Internet Protocol (VoIP)—A telecommunications technology that enables the convergence of voice, data, and video over a common medium. It is not only about telephony, but a wide variety of applications that travel efficiently and seamlessly over private or public Internet Protocol (IP) networks.

Voice Recognition—The conversion of spoken words into computer text. Speech is digitized first then matched against a dictionary of coded wave forms. The matches are converted into text as if the words were typed on the keyboard. Speaker-dependent systems must be trained before using, by taking samples of actual words from the person who will use it.

Voice-Coder (Vocoder)—A device that usually consists of a speech analyzer which converts analog speech waveforms into narrowband digital signals, and a speech synthesizer which converts the digital signals into artificial speech sounds. Vocoders are used to reduce bandwidth requirements for transmitting digitized speech signals.

Volatile Memory—Memory that loses its stored data when power is removed.

Volume Unit (VU)—The unit of measurement for electrical speech power in communications work as measured by a VU meter. Zero VU equals zero dBm (1 milliwatt) in measurements of sine wave test tone power.

Vulnerability Analysis—Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Vulnerability Assessment—Measurement of vulnerability that includes the susceptibility of a particular system to a specific attack and the opportunities available to a threat agent to mount that attack. NOTE: This process may or may not be automated. See Risk Assessment.

Vulnerability—1. Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited. 2. Defense weakness to control a threat to the AIS.

Waveguide—A transmission line comprised of a hollow metallic conductor generally rectangular, elliptical, or circular in shape, within which electromagnetic waves may be propagated.

Wavelength Division Multiplexing (WDM)—In optical fiber communications, a technique that is identical to frequency division multiplexing. The term is applied to the use of different wavelengths for the light signals along an optical fiber.

Wavelength—The length of a electromagnetic or radio wave indicated in meters. It is equal to the distance traveled by the wave in one period of oscillation. Wavelength and frequency are directly related. The wavelength equals the velocity of the wave (generally considered equal to the speed of light) divided by its frequency.

Weapon System—An item or set of items that can be used directly by warfighters to carry out combat or combat support missions, to include tactical communications systems.

Web Cache—In computing, a method to reduce world wide web traffic congestion and improve server response time. A storage area that sits between the web/source servers and the client. It reduces latency on the Internet by satisfying the request form the data in the cache instead of from the source server, taking less time to get and display the object. There are two types of web caches, browser cache and proxy cache.

Web Server—A software program or server computer equipped to offer World Wide Web access. A web server accommodates requests from users, retrieves requested files or applications, and issues error messages.

Webspace—The virtual space created by the World Wide Web or a subset of that space occupied by a particular Web site.

White Noise—In communications-electronics, noise whose frequency spectrum is continuous and uniform over a wide frequency range.

White Pages—1**.** An electronic information database that contains user names and their associated network addresses, in the manner of a telephone directory. 2. In networking, a directory containing the electronic addresses of users organized by user name.

Wide Area Information Server (WAIS)—A distributed information service and search engine that allows natural language input and indexed searching. Many Web search utilities use a WAIS engine.

Wide Area Network (WAN)—1. A system of links that are used to interconnect geographic regions. The WAN normally provides routing, switching, or gateway points to the MANs, LANs, or other WANs. 2. A public or private computer network serving a wide geographical area.

Wideband—That property of a communications facility, system, equipment, or channel in which the range of frequencies used for transmission is greater than 0.1 percent of the center or midband frequency. An imprecise term today which originated in the early days of telecommunications meaning a bandwidth exceeding that of a nominal 4 kHz telephone voice channel. Wideband generally refers to a signal

occupying a wide range (band) of frequencies, typically several hundred MHz. Wideband is also often used to distinguish it from narrowband, where both terms are subjectively defined relative to the implied context; for example, high frequency (HF) radio systems are considered narrowband, while line-of-sight microwave radio and satellite radio communications systems are termed wideband because of the "width" of their transmitted signals. Synonymous with broadband. Also see bandwidth.

Wired Equivalent Privacy (WEP)—A security protocol for wireless local area networks (WLANs). WEP is designed to provide the same level of security as that of a wired LAN; it encrypts data over radio waves.

Wireless—In computer networking, descriptive of a network, terminal, or component that uses electromagnetic waves (typically radio frequency or infra-red waves) rather than wire conductors (cables) to communicate. Wireless devices generally contain both transmitters and receivers to communicate. In general, this term refers to communications via electromagnetic waves.

Wireless Application Protocol (WAP)—1. A specification for a set of communications protocol to standardize the way wireless devices, such as cellular telephones and radio transceivers, can be used for internet access, including e-mail, world wide web (www), etc. WAP is both an application environment and a set of communications protocols for wireless devices designed to manufacturer-, vendor-, and technology-independent access to the Internet and advanced telephony services.

Wireline—A term associated with a computer network or terminal that uses wireline technology (conventional telephone lines) to communicate.

Wiretapping—Attaching an unauthorized device, such as a computer terminal, to a communications circuit to gain access to data by generating false messages or control signals, or by altering legitimate users' communications.

Workstation—1. In automated information systems, the input, output, display, and processing equipment that provides the operator-system interface. 2. A configuration of input, output, display, and processing equipment that constitutes a stand-alone system not requiring external access.

World Wide Web (WWW)—An international, virtual network-based information service composed of internet host computers that provide on-line information in a specific hypertext format. The WWW, called the Web for short, exists virtually and uses the internet to transmit hypermedia documents between computers internationally. No one organization owns the WWW; users are responsible for the documents they author and make available publicly on the Web. The Web refers to a body of information, while the Internet refers to the physical side of the Global network. A distributed Hyper Text-based information system to provide its user community easy access to global information.

World Wide Web Consortium (W3C)—The W3C was created in 1994 to lead the WWW to its full potential by developing common protocols that promote its evolution and ensure its interoperability. The W3C develops interoperable technologies, such as specifications, guidelines, software, and tools. W3C has more than 500 Member organizations from around the world and has earned international recognition for its contributions to the growth of the Web.

Worldwide Coverage—In satellite communications, earth coverage between 65 degrees North and 65 degrees South latitude and at all longitudes.

Worm—A self-contained computer program that replicates itself and is self-propagating; similar to a virus. While viruses are designed to cause problems on a local system and are passed through boot sectors of disks and through files, worms are designed to thrive in network environments.

Write-Once Read-Many (WORM)—In computing, refers to a type of optical memory disk that can be written to once and cannot be erased or formatted.

Write—To transfer information to an output medium. To copy from internal storage to external storage.

X.500 Server—A standard distributed database server system used for a wide range of purposes in the network world.

X.509—A widely-used specification for digital certificates.

X band—In radio communications, the frequency band between 8-12 GHz.

X-Axis—A horizontal axis in a system of rectangular coordinates; that line on which distances to the right or left (east or west) of the reference line are marked, especially on a map, chart, or graph.

X-Y Plotter—In peripherals, a plotting device that receives X- and Y- coordinates from a computer and plots a coordinate graph.

Yagi Antenna—A directional antenna array usually consisting of one driven one-half wave length dipole section, one or more parasitically excited reflectors, and one or more parasitically excited directors. A yagi antenna offers very high directivity and gain.

Yaw—In satellite communications, a rotation of a satellite about an axis that joins the satellite to the center of the earth.

Y-Axis—A vertical axis in a system of rectangular coordinates; that line on which distances above and below (north or south) the reference line are marked, especially on a map, chart, or graph.

Yocto (y)—A prefix used to denote 10^{-24}.

Z-Axis Intercept—In satellite communications, the intersection of a satellite's Z-axis and the earth's surface. It defines an antenna's pointing direction.

Zepto (z)—A prefix used to denote 10^{-21}.

Zero (A Device)—To erase all the data stored in a memory. Synonymous with bit stuffing. The operation of inserting 0-bits in strings of 1-bits to prevent any groups in the user data stream from being interpreted as flags, or, possibly, control characters.

Zero Suppression—In computing, the elimination of zeros to the left of the most significant digits of a number, especially before printing.

Zero Transmission Level Point (0 dBm TLP)—In a communications system, a point in the signal path at which the reference signal power level is 1 milliwatt, that is, 0 dBm. The reference is for system design and test purposes; the actual power level of the communications traffic is not necessarily 0 dBm.

Zerofill—To fill unused storage locations (memory) with the representation of the character denoting 0.

Zeroize—To remove or eliminate the key from cryptoequipment or fill device.

Zeroized—Referring to, or characterized by, electronically stored data that have been degaussed, erased, or overwritten.

Zero-Level Decoder—A decoder that yields an analog level of 0 dBm at its output when the input is the digital milliwatt signal (a 1 kilohertz sine wave).

Zip Cord—In optical communications, a two-fiber cable consisting essentially of two single-fiber cables

having their jackets conjoined by a strip of jacket material.

Zone Beam—In satellite communications, a satellite beam pattern with a footprint that can cover less than 10 percent of the earth's surface.