



DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

DISA CIRCULAR 310-70-1*

APR 21 2012

METHODS AND PROCEDURES

Global Information Grid (GIG) Technical Control

1. **Purpose.** This Circular prescribes policy and provides procedures for Global Information Grid (GIG) technical control.
2. **Applicability.** This Circular applies to the Defense Information Systems Agency (DISA), military departments (MILDEPs), other activities of the Department of Defense (DoD) or governmental agencies, and contractors responsible for the operation and maintenance (O&M) of the GIG.
3. **Authority.** This Circular is published in accordance with the authority contained in DoD Directive 5105.19, Defense Information Systems Agency (DISA), 25 July 2006.
4. **References.**
 - 4.1 DISA Circular (DISAC) 310-55-1, Status Reporting, 21 January 2000.
 - 4.2 DISAC 310-70-57, Defense Information System Network (DISN) Quality Assurance (QA) Program, 20 May 2009.
 - 4.3 DISAC 310-55-9, Base Level Support for the Defense Information System Network (DISN), 5 November 1999.
 - 4.4 DISAC 300-175-9, Global Information Grid (GIG) Operating-Maintenance Electrical Performance Standards, 8 June 1998.
 - 4.5 DISAC 310-130-2, Management Thresholds and Performance Objectives, 21 April 2000.
 - 4.6 DISAC 310-130-1, Submission of Telecommunications Service Requests, 4 April 2000.

4.7 DISAC 310-130-4, Defense User's Guide to the Telecommunications Service Priority (TSP) System, 8 September 1997.

4.8 Supplement 1 to DISAC 310-70-1, DII Technical Control Test Descriptions, 8 May 1998.

4.9 DISAC 310-65-1, Circuit and Trunk File Data Elements and Codes Manual of the Global Information Grid (GIG), 25 April 2002.

4.10 DISAC 310-D70-30, Global Information Grid (GIG) National Gateway Center (NGC) and Subscriber Operations, 21 April 2001.

4.11 DISA-Defense Information Technology Contracting Organization (DITCO) Circular 350-135-1, Defense Commercial Communications Acquisition Procedures, 12 February 1996.
<https://www.ditco.disa.mil/corporatelibrary/>.

5. Definitions and Glossary of Terms. Definitions and a glossary of terms follow the table of contents.

6. Policy. This Circular is the governing directive for exercising transmission control of GIG links, trunks, and circuits by the GIG Facility Control Offices (FCOs), Technical Control Facilities (TCFs), and Patch and Test Facilities (PTFs) operating at levels 3, 4, and 5 in the Defense Information Systems Agency (DISA) system control hierarchy.

7. Relationship to Other Publications.

7.1 The procedures contained in this Circular are to be used in conjunction with all Service publications or other directives regarding control of GIG transmission facilities, links, trunks, and circuits.

7.2 Technical control personnel must be familiar with related Allied Communications Publications (ACPs) and other DISA Circulars and MILDEP regulations, technical manuals, and technical orders that contain detailed and specific information necessary for effective and efficient operations of GIG facilities.

8. Supplemental Procedures. Any supplemental procedures to this Circular must be submitted to DISA, ATTN: Principal Director for Operations (GO), P.O. Box 549, Fort Meade, MD 22705-0549, for approval prior to publication.

9. **Procedural Changes.** All DISA activities, MILDEPs, and O&M elements are invited to submit recommended changes to this Circular. The recommendations are to be forwarded through the appropriate DISA Theater Network Operations Center (TNC) to DISA, ATTN: Principal Director for Operations (GO), P.O. Box 549, Fort Meade, MD 20755-0549, with an information copy to the appropriate O&M headquarters.

FOR THE DIRECTOR:



LORI L. RAMIREZ
Chief of Staff (Acting)

SUMMARY OF SIGNIFICANT CHANGES. This revision redefines reporting hierarchy and roles and responsibilities of the Facility Control Offices (FCOs). A training plan was added in chapter 2. The aspects of Transmission Monitoring Control (TRAMCON) and Digital Patch and Access System (DPAS) were deleted with the removal of chapter 3. The aspect of authorized service interruptions (ASIs) was deleted with the removal of chapter 7.

*This Circular cancels DISAC 310-70-1, 25 June 1998.

OPR: GO53

DISTRIBUTION: W

Return to:

[Top of Basic Circular](#)

Continue to:

[Top of Table of Contents](#)

[DISA Publication Listing](#)

[DISA Home Page](#)

DISA PUBS@disa.mil - Last revision: 21 March 2012

CONTENTS

BASIC CIRCULAR

1. Purpose
2. Applicability
3. Authority
4. References
5. Definitions and Glossary of Terms
6. Policy
7. Relationship to Other Publications
8. Supplemental Procedures
9. Procedural Changes

C1. CHAPTER 1. DEFENSE INFORMATION SYSTEMS AGENCY (DISA)

- C1.1 Authority and Mission
- C1.2 Global Information Grid (GIG)
- C1.3 Defense Information System Network (DISN)
- C1.4 GIG Reporting Hierarchy
- C1.5 Reporting Responsibilities
- C1.6 Operating Messages
- C1.7 Orderwires

C2. CHAPTER 2. GIG CONTROL FACILITIES AND PERSONNEL

- C2.1 General
- C2.2 Configuration Concept and Criteria
- C2.3 Functions and Duties of a Facility Control Office (FCO)
- C2.4 Functions and Duties of a GIG Technical Control Facility (TCF)
- C2.5 Functions and Duties of a GIG Patch and Test Facility (PTF)
- C2.6 Additional Functions and Duties of TCF or PTFs
- C2.7 Operational Control of Maintenance Support
- C2.8 Technical Controller Skills and Knowledge
- C2.9 Facility Qualification Training
- C2.10 Familiarization and Coordination Visits
- C2.11 Duties of GIG Users

- C3. Omitted

C4. **CHAPTER 4. GIG TRANSMISSION NETWORKS**

- C4.1 General
- C4.2 Bulk Encryption

C5. **CHAPTER 5. CONTINGENCY OPERATIONS**

- C5.1 General
- C5.2 Telecommunications Service Priority (TSP)
- C5.3 Minimum Essential Circuit List (MECL)
- C5.4 On-call Service
- C5.5 Tactical Circuits

C6. **CHAPTER 6. QUALITY CONTROL**

- C6.1 General
- C6.2 In-Service Performance Monitoring
- C6.3 Out-of-Service Testing
- C6.4 Trend Analysis
- C6.5 Test Tone Power Levels
- C6.6 Excessive Signal Levels
- C6.7 Test and Acceptance (T&A) Testing
- C6.8 Equipment Test and Acceptance Test
- C6.9 Waivers

C7. Omitted

C8. **CHAPTER 8. SERVICE PROVISIONING**

- C8.1 General
- C8.2 Telecommunications Service Order (TSO)
- C8.3 Circuit Installation, Alignment, Testing, Certification, and Deactivation
- C8.4 Completion Reports

C9. **CHAPTER 9. ADMINISTRATION**

- C9.1 General
- C9.2 Automated Recordkeeping
- C9.3 Required Forms
- C9.4 Service Provisioning Records
- C9.5 Reference Library

C10. **CHAPTER 10. COMMERCIALY LEASED CIRCUITS**

- C10.1 General
- C10.2 Categories

- C10.3 Meeting and Maintaining Technical Sufficiency
- C10.4 Initial Acceptance of Leased Service
- C10.5 Circuit Problems
- C10.6 TCF and PTF Cooperation with Commercial Carriers
- C10.7 Scheduled Outages
- C10.8 Impaired Service
- C10.9 Quality Control (QC) Testing
- C10.10 Outage Reporting

ILLUSTRATIONS

Figure

- F1.1 GIG Reporting Hierarchy
- F2.1 Sample GIG User Notification Memorandum
- F5.1 TSP Identification Code
- F6.1 Network Element Performance Monitoring
- F6.2 Q Parameter Segmented Testing
- F8.1 Sample Telecommunications Service Order (TSO)
- F8.2 Sample In-Effect Report (IER)
- F8.3 Sample Exception Report
- F8.4 Sample Delayed Service Report (DSR)
- F8.5 Sample Ready For Use (RFU) Report

Table

- T6.1 Analog Circuit Quality Control Test Schedule
- T6.2 Digital Circuit Quality Control Test Schedule

Return to:

[Top of Table of Contents](#)
[Basic Circular](#)

Continue to:

[Chapter 1](#)
[DISA Publication Listing](#)
[DISA Home Page](#)

DISA PUBS@DISA.MIL - Last change: 21 March 2012

DEFINITIONS AND GLOSSARY OF TERMS

Combatant Commanders. The combatant commanders have geographic area responsibilities. These combatant commanders are each assigned an area of responsibility (AOR) by the Unified Command Plan (UCP) and are responsible for all operations within their designated areas: U.S. Joint Forces Command, U.S. Central Command, U.S. European Command, U.S. Pacific Command, and U.S. Southern Command. There are four combatant commanders assigned worldwide functional responsibilities not bounded by geography: U.S. Space Command, U.S. Special Operations Command, U.S. Strategic Command, and U.S. Transportation Command.

Communications Facility. A facility normally operated and maintained by an operations and maintenance (O&M) that provides some communications service and has at least one circuit terminating or passing through the facility.

Continuity of Operations (COOP). An effort within individual organizations (e.g., Federal executive branch departments and agencies) to ensure that Mission Essential Functions (MEFs) and Primary Mission Essential Functions (PMEFs) continue to be performed during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies.

Critical Control Circuits (CCC). Voice and data communications circuits used by the DISA Network Operations Center (DNC) for operational direction and exchange of Global Information Grid (GIG) status information between DNC elements and between the DNC and GIG technical control, traffic switching or relay facilities, satellite facilities, and other GIG operating elements. CCCs represent DISA requirements and are subject to the validation of the Director, DISA.

DISA Command Center (DCC). Exercises the authority of the Director, DISA, providing command and control (C2) of DISA's current operations to support DoD and national leadership. DISA provides assured enterprise capabilities and services across the full spectrum of operations in an environment in which both the nature of the threat and the method of warfare continue to change. Because of asymmetric challenges inherent to irregular warfare, DoD requires an agile communications, computing, and services foundation that supports the necessary ad hoc, on-demand responses to these threats. DISA's strategy, as stated in the Campaign Plan, reflects this reality as

DISA pursues three lines of operation (LOOs): Enterprise Infrastructure, Command and Control and Information Sharing, and Operate and Assure. The DCC is level 1 of the GIG Systems Hierarchy.

DISA Network Operations Center (DNC). Exercises day-to-day operational direction over the GIG control facilities, GIG voice and data traffic switching facilities, satellite facilities, and other GIG operating elements, either directly or indirectly, through its subordinate regions within the assigned geographical area. The DNCs provide technical support and execution and are tactical control (TACON) for Theater NetOps issues to combatant commands for those parts of the GIG under their control. The DNCs act as the theater focal point to maintain NetOps situational awareness, support the combatant commands in executing their GIG responsibilities, and serve as liaison between a Theater Command, Control, Communications, and Computers (C4) Control Center (TCCC) or Global C4 Control Center (GCCC) and the DISA Command Center (DCC). Each DNC is responsible for the effective operation and defense of the GIG within the theater and for providing onsite, theater support for NetOps, as referenced in the Joint Concept of Operations (CONOPS) for GIG NetOps.

End-to-End. As used in Circular, end-to-end refers to the total circuit path, as prescribed in the Telecommunications Service Order (TSO), from the terminal equipment at one end to the terminal equipment at the far end.

Enhanced Mobile Satellite Services (EMSS). Provides satellite-based telephone and data communication service, utilizing a commercial satellite infrastructure to provide voice and low data rate services from a mobile, lightweight handset through a DpD dedicated gateway which accesses the Defense Information System Network (DISN). EMSS is capable of providing Type-1 secure voice service and non-secure access to commercial and Defense Switched Network (DSN) telephone services.

Facility Control Office (FCO). Responsible for day-to-day operation and maintenance (O&M) of Global Information Grid (GIG) facilities within a designated geographical area. FCOs are staffed and equipped by O&M activities and are assigned level 3 responsibilities in the system control hierarchy. FCOs are manned 24 hours a day and must have sufficient communications connectivity (to include a secure means) to fulfill the functions and responsibilities contained in DISAC 310-70-1.

GIG Infrastructure Services Management Center (GISMC).

The primary DoD enterprise level applications services NetOps center that supports the DISA Network Operations Centers (DNCs) with applications layer network and systems management, visibility, monitoring, analysis, planning, and control. The center optimizes the integrated NetOps of the existing and emerging applications networks and services as referenced in the Joint CONOPS for GIG NetOps.

Global Information Grid (GIG). The definition of GIG, was established in a DoD Chief Information Officer (CIO) memorandum, dated 22 September 1999, which, which subsequently was revised on 2 May 2001, by agreement among the DoD CIO, Under Secretary of Defense (USD) for Acquisition Technology and Logistics (AT&L), and the Joint Staff/J6. The GIG is defined (Source: GIG Capstone Requirements Document, JROCM 134-01, 30 August 2001) as follows:

The Global Information Grid (GIG) is an all-encompassing communications project of the United States Department of Defense. It is defined as a "globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel."

The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems (NSS). Non-GIG information technology (IT) includes stand-alone, self contained, or embedded IT that is not, and will not be, connected to the enterprise network. This new definition removes references to the National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. Further, this new definition removes the references to the GIG providing capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). And lastly, this definition removes the part of the definition that discusses the interfaces to coalition, allied, and non-Department of Defense users and systems.

The DoD's use of the term "GIG" is undergoing changes as the Department deals with new concepts; such as, Cyberspace Operations, GIG 2.0 (A Joint Staff J6 Initiative) and the Department of Defense Information Enterprise (DIE). The GIG is managed by a construct known as Network Operations (NetOps).

NetOps is defined as the operational framework consisting of three essential tasks, situational awareness (SA), and command and control (C2) that the Commander of U.S. Strategic Command (USSTRATCOM), in coordination with DoD and Global NetOps community, employs to operate and defend the GIG to ensure information superiority.

Global Information Grid Facility (GIG Facility). Government-owned or a combination of government-owned, fixed, transportable, mobile assets or leased equipments, as appropriate, that provide general purpose, long haul, point-to-point transmission media system, traffic switching function, or communications support capability. The GIG facility can support requirements via DISN, GIG, or other DoD service specific transport or service assets and is an essential means for the customer to interface their requirement with Government-Furnished Equipment (GFE) communications assets to provide the connectivity and or service typically based on Telecommunications Service Orders (TSOs). The facility is normally operated and maintained by the Government or a contractor through which or to which GIG or a combination of GIG/non-GIG communications links, trunks, or circuits pass or terminate. The GIG facility can accomplish a variety of functions including terrestrial or satellite transmission, message switching, circuit switching, circuit restoration, rerouting, trouble isolation, repair, circuit coordination, or facility coordination. A communications facility is not considered GIG facility until such time as the site has been commissioned by appropriate DISA Quality Assurance personnel, per DISAC 310-70-57, DISN Quality Assurance.

Information Technology (IT). Any equipment, or interconnected system(s) or subsystem(s) 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 agency.

Intermediate Control Office (ICO). If the layout of a circuit or trunk is such that the overall Communications Control Office (CCO) is not in the best position to perform tests and coordinate the activities of some of the intermediate TCFs, another TCF may be designated as an ICO. ICOs will be designated in the TSO at the time the layout is placed in effect and will assume the responsibility for the general service condition of the assigned segment. Temporary ICOs may be designated by the appropriate TSO issuing authority for the specific purpose of completing TSO change actions. Otherwise, the CCO assigned

to the circuit will be designated in the TSO to effect the change. ICOs are responsible to the CCO for operational direction.

International Maritime Satellite (INMARSAT). Established in 1979 to serve the maritime industry by developing satellite communications for ship management and distress and safety applications. It has since expanded into land, mobile, and aeronautical communications, so that users now include thousands of people who live or work in remote areas without reliable terrestrial networks or travelers anywhere. In addition to maritime customers, today's typical users include journalists and broadcasters, health teams and disaster relief workers, land transport fleet operators, airlines, airline passengers and air traffic controllers, government workers, national emergency and civil defense agencies, and heads of state.

Interswitch Trunk (IST). A trunking circuit between switching centers. For example, in the Defense Switched Network (DSN), an IST is any trunking circuit that connects two DSN multi-functions switches together.

Joint Hawaii Information Transfer System (JHITS). Provides enhanced information transfer capabilities to DoD and certain other authorized users in the State of Hawaii, defined to be the eight primary islands. The JHITS provides a full range of GIG compliant end-to-end switched voice, video, data and DISN transmission services for both the backbone as well as for the infrastructure of the base, post, camp and station.

Management Control. The review, evaluation, coordination, and guidance of management actions necessary to fulfill the responsibility of operational direction of the Global Information Grid (GIG).

Monitoring Center (MC). Located at a GIG control facility where one or more trunks terminate or where remotely controllable testing access to all derived channels exists. The MC exercises technical supervision over switching centers and assigned trunks to the distant end facilities where the trunks break out into individual channels. The MC is responsible for initial activation, acceptance of leased trunks on behalf of the U.S. Government, and submission of appropriate completion reports required by the TSO issuing authority. The MC is also responsible for coordinating realignment of the trunk when necessary to maintain end-to-end engineered values stated in the Telecommunications Service Order (TSO).

Near-Term. Where "real-time" is the time it takes to react to a situation, "near-term" is a longer period of time in which analyses and more permanent corrective actions are initiated.

Network. An interrelated organization of devices, workstations, switching centers, or facilities tied together to serve a common purpose, capable of intercommunicating.

Network Control. Provides real-time and near-term control of switched or special networks; reconstitution, restoral, and extension supervision; satellite system and payload control; and resource allocation.

Network Management. A set of procedures, equipment, and operations designed to keep a network operating near maximum efficiency when unusual loads or equipment failures would otherwise force the network into a congested, inefficient state.

Network Management Center. A centralized control center from which a specific network is monitored and controlled and statistical information is collected.

Operating Elements of the GIG. A control center staffed and equipped by O&M activities that exercises responsibilities at levels 3, 4, or 5 of the GIG system control hierarchy.

Operation and Maintenance (O&M) Elements (O&M Activities). Military department (MILDEP), Department of Defense (DoD), or contracted elements that are responsible for the O&M for a GIG facility or system.

Operational Direction. Operational direction includes authority to direct the operating elements of the GIG, assign tasks to those elements and supervise the execution of those tasks; allocate and reallocate GIG facilities to accomplish the mission; and develop technical standards, practices, methods and procedures for the performance and operation of the Global Information Grid (GIG).

Orderwire. Traditionally those voice and data telecommunications circuits (to include teletype) used for exchange of surveillance and control information between operating elements of the GIG. For the purposes of the Circular, orderwire is the term used to describe mission critical alternate means of communications between DISN sites serviced by government owned transport.

Patch and Test Facility (PTF). The part of a GIG facility that functions as a supporting activity normally under the technical supervision of a Technical Control Facility (TCF). A PTF has the same functions and responsibilities as a TCF with the exception that the physical and electrical capabilities may be limited. A PTF is a facility which normally supports one major user or several minor users; is the 2d, 3d, 4th, etc. control facility in a geographical location (GEOLOC) that reports to a TCF; may or may not be manned 24 hours a day; can access some circuits and trunks traversing the facility for purposes of monitoring, testing, and restoral; has some testing capabilities; may or may not be able to restore major equipment components.

Serving Technical Control and or Patch and Test (TCF and or PTF). Provides direct interface between local users and the GIG. The serving TCF and PTF is responsible for coordination with the user and ensuring complete end-to-end service for that user.

System Control. Ensures user-to-user service is maintained under varying network traffic conditions, fluctuating user requirements, natural or manmade stresses and disturbances, and equipment failures or degradations. It includes the interrelated activities of facility surveillance, traffic surveillance, network control, traffic control, and technical control. System control facilities include the DISA control centers, operation and maintenance (O&M) technical control facilities, and other facilities that are capable of providing system control at all levels of the hierarchy.

Systems Management Center (SMC). Creates points of convergence for problem resolution and forms a gateway to aid in facilitating customer support requirements for accessing and using the information technology (IT) products and services provided by the Computing Services Directorate (CSD). The SMC provides operational management oversight, support, and problem resolution for production environments. The SMC is realigned into primary areas reporting to a single Director or Commander, as described in the Defense Information Systems Agency Network Operations Concept of Operations (DISA NETOPS CONOPS).

Technical Control (Tech 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. This also includes direction of activities in any work area of the GIG station containing distribution frames and associated jacks or switches through which equipment and facilities are patched or switched to provide the required transmission path. The work areas also include any test equipment or testing capability.

Technical Control Facility (TCF). The part of a GIG station that functions as the interface between the transmission elements of the GIG and the users of the system. It has the physical and electrical capabilities necessary to perform the required functions of technical control described in this Circular. A TCF is a facility which supports more than one major user and is normally manned 24 hours a day; can access all circuits and trunks traversing the facility for purposes of monitoring, testing, and restoral; has complete testing capabilities; and can restore major equipment components (i.e., receivers, transmitters, multiplexers, etc.).

Telecommunications Request (TR). A valid, approved, and funded telecommunications requirement prepared utilizing DISA Direct Order Entry (DDOE) and submitted to DISA or DISA activities for fulfillment. A telecommunications request may only be issued by a specifically authorized Technical Control Office (TCO).

Traffic Control. Provides real-time and near-term control of traffic flow and routing; such as, code cancellation, code blocking, alternate route cancellation, line load control, and user prioritization.

Traffic Surveillance. Traffic surveillance provides real-time data concerning systems and network loading, data processing queue status, message backlog, and buffer-fill-rate data and other measures to describe system, network, and facility congestion and traffic load. It also includes associated near-term data reduction and analysis to support traffic control. It provides data to support mid- and long-range system management engineering, operation, and maintenance.

Unified Command Plan (UCP). The document that sets forth basic guidance to all combatant commanders. The UCP establishes combatant command missions, responsibilities, and force structure; delineates geographic areas of responsibility for geographic combatant commanders; and specifies functional responsibilities for functional combatant commanders. The unified command structure generated by the UCP is flexible and changes as required to accommodate evolving U.S. national

security needs. Title 10 USC 161 tasks the Chairman of the Joint Chiefs of Staff (CJCS) to conduct a review of the UCP "not less often than every two years" and submit recommended changes to the President through the Secretary of Defense.

Wideband Satellite Communications (SATCOM) Operations Center (WSOC). The WSOC exercises day-to-day operational payload management and control of Defense Satellite Communications System (DSCS) and Wideband Global SATCOM (WGS) satellites.

| | |
|----------|---|
| A&E | allocation and engineering |
| AC | air conditioning |
| ACP | Allied Communications Publication |
| ADP | automatic data processing |
| AE | advance encryption |
| AFNOSC | Air Force Network Operations Service Centers |
| AGNOSC | Army Global Network Operations Service Centers |
| ALLA | Allied Long Lines Agency |
| AMHS | Automatic Message Handling System |
| AMI | Alternate Mark Inversion |
| AOR | area of responsibility |
| ASD(C3I) | Assistant Secretary of Defense for Command, Control, Communications, and Intelligence |
| ASI | authorized service interruption |
| ATM | asynchronous transfer mode |
| | |
| BERT | bit error rate test |
| BMDS | Ballistic Missile Defense System |
| | |
| C2 | command and control |
| C3 | critical control circuits |
| CCCI | Central Conference Communication Initiative |
| CCO | Communications Control Office |
| CCSD | command communications service designator |
| | |
| CHNL | channel |
| CLR | circuit layout record |
| CMO | Communications Management Office |
| COMSEC | communications security |
| CONUS | continental United States |
| COOP | continuity of operations |
| CRP | completion report |
| CSA | communications service authorization |
| CT | current transformer |

| | |
|--------|---|
| DATMS | DISN Asynchronous Transfer Mode Services |
| DCC | DISA Command Center |
| DD | Department of Defense |
| DDOE | DISA Direct Order Entry |
| DGIS | DoD Gateway |
| DHS | Department of Homeland Security |
| DII | Defense Information Infrastructure |
| DISA | Defense Information Systems Agency |
| DISAC | DISA Circular |
| DISN | Defense Information System Network |
| DITCO | Defense Information Technology Contracting Organization |
| DMS | Defense Message System |
| DNC | DISA Network Operations Center |
| DoD | Department of Defense |
| DOR | detailed outage report |
| DOV | Disbursing Office Voucher |
| DSCS | Defense Satellite Communications System |
| DSN | Defense Switched Network |
| DSR | delayed service report |
| DTG | date time group |
| DWDM | dense wavelength division multiplexing |
| EFS | error free seconds |
| ERS | emergency relocation site |
| ETR | estimated time of return |
| FAC | facility |
| FaCIT | facility and circuit information tracking |
| FCC | Federal Communications Commission |
| FCO | Facility Control Office |
| FDDI | Fiber Distributed Data Interface |
| GCM | GIG Content Management |
| GEM | GIG Enterprise Management |
| GEOLOC | geographical location |
| GFE | government-furnished equipment |
| GIG | Global Information Grid |
| GNC | Global Network Center |
| GND | GIG Network Defense |
| GNOSC | Global Network Operations Service Center |
| GO | DISA Operations Directorate |
| GO6 | Gateway/SATCOM Operations Division |
| GPS | global positioning system |
| HAZCON | hazardous condition |
| HDLC | high-level-data-link-control |

| | |
|----------|--|
| HF | high frequency |
| HQ | headquarters |
| HSGR | High Speed Global Ring |
| ICO | Intermediate Control Office |
| ID | identification |
| IER | in-effect report |
| IFCO | Intermediate Facility Control Office |
| INT | initials |
| IP | internet protocol |
| IPN | impulse noise |
| ISDN | Integrated Services Digital Network |
| IST | interswitch trunk |
| IT&A | initial test and acceptance |
| ITU-T | International Telecommunication Union - Telecommunication |
| JHITS | Joint Hawaii Information Transfer System |
| JWICS | Joint Worldwide Intelligence Communications System |
| Ka-STARS | Ka-Band Satellite Transmit and Receive System |
| LANs | Local Area Networks |
| LRP | local restoral plan |
| MAP | Multiprotocol Label Terminal |
| MC | Monitoring Center |
| MCNOSC | Marine Corps Network Operations Service Center |
| MECL | minimum essential circuit list |
| MILDEP | military department |
| MIL-HDBK | military handbook |
| MIL-STD | Military Standard |
| MSL | Master Station Log |
| MT | management threshold |
| NA | not assigned |
| NAVGNOSC | Navy Global Network Operations Service Center |
| NBR | number |
| NCS | National Communications System |
| NDB | no data base entry |
| NE | network element |
| NetOps | network operations |
| NGC | National Gateway Center |
| NMC | Network Management Center |
| NOSC | Network Operations Service Center |
| NRZ | non-return-to-zero |
| NSC | Node Site Coordinator |

| | |
|---------|---|
| O&M | operation and maintenance |
| O&M PT | operation and maintenance patch and test |
| OCM | Operational Coordination Message |
| OCONUS | outside continental United States |
| ODM | Operational Direction Message |
| OPCON | operational control |
| OPSEC | operations security |
| OSI | open system interconnection |
| | |
| PAT | Precedence Access Threshold |
| PCE | Port Channel Engineering |
| PCM | pulse code modulation |
| PDC | Program Designator Code |
| PE | performance evaluation |
| PMP | Performance Monitoring Program |
| POC | point of contact |
| POP | Points of Presence |
| PTF | Patch and Test Facility |
| | |
| QA | quality assurance |
| QC | quality control |
| | |
| RADAY | radio day |
| RCV | receive |
| RFO | reason for outage |
| RFU | ready for use |
| R-Plans | restoral plans |
| | |
| SA | situational awareness |
| SAM | Status Acquisition Message |
| SATCOM | satellite communications |
| SCO | System Control Officer |
| SDB | sequence data base |
| SDLC | synchronous-data-link-control |
| SND | send |
| SOP | standard operating procedure |
| SR | service request |
| SRM | Switch Revision Message |
| STM | system trace |
| | |
| T&A | test and acceptance |
| TCCC | Theater C4 Control Center |
| TCF | Technical Control Facility |
| TCOSS | Telecommunications Certification Office Support System |
| TDM | time division multiplexing |

TIB tactical interface box
TIP Tactical Interface Point
TLP transmission level point
TNC Theater Network Operations Center
TR Telecommunications Request
TLP transmission level point
TSO Telecommunications Service Order
TSP Telecommunications Service Priority
TSR Telecommunication Service Request

USCENTCOM United States Central Command
USEUCOM United States European Command
USIC United States international carrier
USNORTHCOM United States Northern Command
USPACOM United States Pacific Command
USSOUTHCOM United States Southern Command
USSTRATCOM United States Strategic Command

VF voice frequency

WAN Wide Area Network
WSOC Wideband Satellite Communications (SATCOM)
Operations Center
WWOLS World Wide Online System

Return to:

[Top of Table of Contents](#)
[Basic Circular](#)

Continue to:

[Chapter 1](#)
[DISA Publication Listing](#)
[DISA Home Page](#)

DISA PUBS@DISA.MIL - Last change: 21 March 2012

C1. CHAPTER 1. DEFENSE INFORMATION SYSTEMS AGENCY (DISA)

C1.1 Authority and Mission.

C1.1.1 DoD Directive 5105.19 established the Defense Information Systems Agency (DISA) as a Combat Support Agency of the Department of Defense (DoD) under the direction, authority, and control of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) and provides the authority to conduct its mission.

C1.1.2 DISA shall be responsible for planning, engineering, acquiring, testing, fielding, and supporting global net-centric information and communications solutions to serve the needs of the President, Vice President, Secretary of Defense, and DoD Components, under all conditions of peace and war.

C1.2.2.1 DISA supports national security communications requirements, as identified in the National Security Presidential Directive--28, "United States Nuclear Weapons Command and Control, Safety, and Security," and Executive Order 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions," as amended. DISA DoD transport services are used for voice, data, and video services through a combination of terrestrial and satellite assets and services.

C1.2.2.2 DISA provides enterprise-level development, integration, and management services for interagency, strategic, allied, multinational, coalition, joint and combined command and control (C2), and combat support capabilities. DISA works, in conjunction with other DoD Components, to ensure the security of DoD enterprise systems and supports the commanders of the combatant commands and deployed forces by designing and deploying proactive protections, deploying attack detection, and performing other necessary security functions. DISA provides and or hosts legacy and net-centric enterprise services, main-frame and server computer operations, Web services, production support, technical services, and end user assistance for C2, combat support, and eBusiness functions throughout DoD. DISA supplies standards, interoperability testing, spectrum support and solutions, and integrated architecture development for the DoD net-centric enterprise information environment. DISA provides the DoD enterprise with a net-centric, service-based, shared enterprise infrastructure that supports ubiquitous

user access to reliable capabilities and decision-quality information. DISA provides enterprise-wide systems engineering support for the GIG to ensure it is planned, acquired, operated, maintained, managed, and improved effectively and efficiently for end-to-end interoperability down to the tactical edge.

C1.2 Global Information Grid (GIG).

C1.2.1 The GIG is a composite of DoD-owned and DoD-leased telecommunications subsystems and networks, as prescribed in DoD Directive 5105.19 (authority document). GIG components include fixed, transportable, and leased equipment that provide long-haul transmission media, traffic switching or relay functions, or communications support capability including assets of the Wideband Satellite Communications (SATCOM) Operations Center (WSOC).

C1.2.2 Recommendations by DISA or other DoD activities for identifying communications facilities as GIG facilities require commissioning, review and approval by the appropriate unified command, and a review of the appropriate component command. If a communications facility or system being considered for inclusion in the GIG meets the component criteria but does not meet established GIG interface, commissioning, installation, or engineering standards (e.g., facilities designed for tactical applications), the unified command and DISA Operations Directorate (GO) will approve the inclusion on an excepted basis. Such exception does not relieve responsible elements from upgrading facilities and equipment to meet GIG standards as resources and funding permit. More information on identifying a facility as a GIG facility can be obtained from the local Defense Information System Network (DISN) Quality Assurance (QA) Office. Once a communications facility is designated as a GIG facility, the GIG facility is then responsible for ensuring appropriate reports are submitted to DISA, in accordance with DISAC 310-55-1, Status Reporting (reference 4.1), as well as being subject to periodic performance evaluations (PEs), in accordance with DISAC 310-70-57, Defense Information System Network (DISN) Quality Assurance (QA) Program, (reference 4.2).

C1.3 Defense Information System Network (DISN). DISA has been directed by the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer(ASD(NII)/DoD CIO) to develop and implement the DISN program to provide a cost effective, efficient, and interoperable information system network for DoD. Each of the individual military service and DoD agency telecom-munications

networks (e.g., Automated Technical Control Programs, Ka-Band Satellite Transmit and Receive System (Ka-STARS), Tactical Interface Point (TIP), Ballistic Missile Defense System (BMDS), Joint Worldwide Intelligence Communications System (JWICS), and High Speed Global Ring (HSGR) will be integrated into global network operations under the management control and operational direction of DISA. Integration of the networks and establishment of Network Management Centers (NMCs) are now known as DISA Network Operations Centers (DNCs).

C1.4 GIG Reporting Hierarchy. The current GIG reporting hierarchy is structured within five hierarchical levels, as depicted in figure F1.1. The first level has operational control (OPCON) over the other four levels. The second level is DISA operated and staffed while the remaining three levels are operated and staffed by the operation and maintenance (O&M) agencies. The exception is that the Network Operations (NetOps) Centers are operated and staffed by the O&M personnel of the Service, Agency, or Command. NetOps is the operational framework consisting of three essential tasks: GIG Enterprise Management (GEM), GIG Network Defense (GND), and GIG Content Management (GCM). These essential tasks provide C2 and situational awareness to the Commander, United States Cyber Command (USCYBERCOM). Thorough coordination within the NetOps community employs operating and defending the GIG ensuring information superiority. Though NetOps is not a direct part of the systems hierarchical chain, the NetOps community along with the entities within the systems hierarchy help to create net centrality of the GIG. The O&M elements at GIG reporting levels 3, 4, and 5 include Facility Control Offices (FCOs), Technical Control Facilities (TCFs), Patch and Test Facilities (PTFs), DISN Points of Presence (POPs), and satellite earth terminals and gateways. The day-to-day flow of information, such as status reporting and coordination, is accomplished through each GIG systems level depicted by the solid lines in figure F1.1. However, when situations dictate, immediate operational control may flow from the GIG systems levels 1 or 2 directly to DISN elements operating at GIG systems levels 3, 4, or 5.

C1.4.1 Level 1: DISA Command Center (DCC). Worldwide control of the GIG is exercised at the DCC. The DCC is directly responsible for managing, controlling, and monitoring various networks; such as, the internet protocol (IP) router networks, Defense Switched Network (DSN), Wideband Satellite Communications (SATCOM) Operations Center (WSOC), and Defense

Information System Network (DISN). The DCC is supported by the DNC staff.

C1.4.2 Level 2: DISA Network Operations Centers (DNCs). Operational control and direction within the continental United States (CONUS), Southwest Asia, Pacific, and European theaters are provided by the established DNCs to enhance system survivability under DISA level 2. Each DNC has a designated continuity of operations (COOP) site, or emergency relocation site (ERS), for contingency operations. The DNC also becomes the operations manager for the combatant commander when the combatant commander assumes temporary operational control of DISA field organizations under their area of responsibility (AOR). The DNC also performs WSOC management actions for the satellites and earth terminals within their area. The DNC CONUS performs the same basic responsibilities as detailed for level 2; however, in addition, the DNC also handles the intertheater connectivity among United States Northern Command (USNORTHCOM), United States Pacific Command (USPACOM), United States European Command (USEUCOM), United States Southern Command (USSOUTHCOM), and United States Central Command (USCENTCOM) AORs.

C1.4.3 Level 3: Facility Control Office (FCO). FCO control is the highest level of O&M control for GIG technical controls. An FCO is designated by each DNC to provide operational control and technical supervision over level 4 and 5 GIG facilities within a designated geographical area. An FCO reports directly to the DNC. The control structure parallels the DISA reporting system to provide a logical flow of operational and technical information between the FCO and subordinate facilities. Military service boundaries will not restrict an FCO in fulfilling its responsibilities. An FCO can be assigned at Service, theater, or regional offices. In AORs, such as DISA CONUS, where an FCO entity has not been utilized for some time, these duties fall upon the Node Site Coordinators (NSCs) of those facilities and technical controls.

C1.4.4 Level 4: Technical Control Facility (TCF). A TCF operates at DISA level 4 where O&M functions are performed on GIG transmission links, trunks, and circuits. A TCF must have the physical and electrical capabilities, in accordance with Military Standard (MIL-STD)-188-154, Subsystem, Equipment, and Interface Standards for Common Long Haul and Tactical Technical Control Facilities, necessary to perform all technical control

functions prescribed by this Circular. A TCF reports directly to the designated FCO. In cases where an FCO has not been designated, the TCF will report directly to the appropriate TNC and NSC. In cases where an FCO has not been designated, the TCF will report directly to the DISA Global Network Center (GNC) or appropriate TNC and NSC.

C1.4.5 Level 5: Patch and Test Facility (PTF), DISN Point of Presence (POP), and Satellite Earth Terminal. The last level of control normally associated with a specific function is a level 5 facility. In many cases, a PTF serves one specific user. Level 5 facilities may have the physical and electrical capabilities of a TCF; however, some of these capabilities (i.e., manning, patching, testing, etc.) may be limited. A PTF and other GIG facilities normally report directly to a designated GIG TCF within the geographical location (GEOLOC). In some locations, a DISN POP (e.g., location with DISN PROMINA or asynchronous transfer mode (ATM) transport) may not report directly to a TCF, particularly when the transport is monitored and controlled from a GIG systems level 2 facility. When there is a GIG TCF within the geographical area, the DISN POP personnel must coordinate any actions concerning the GIG with the TCF. Furthermore, they must advise the TCF whenever any of the conditions contained in this Circular or DISAC 310-55-1 (reference 4.1) occur. Within the DISN POPs, there are NSCs, in accordance with DISAC 310-55-9, Base Level Support for the Defense Information System Network (DISN) (reference 4.3), which handle the same basic, functional circuit specific requirements that the PTF would perform; however, they are also hands-on transport technicians when required by the DNC to assist in troubleshooting transport specific issues. Satellite earth terminals and gateways normally report directly to a GIG PTF that is colocated with the satellite earth terminals and gateways. Otherwise, they report to a designated GIG TCF or directly to the TNC and NSC as well as the WSOC. The satellite earth terminals, gateways, WSOC, and DISA Operations Directorate (GO) Gateway/SATCOM Operations Division (GO6) are only within the systems hierarchy as relevant to GIG and or DISN operations. These entities will otherwise follow SATCOM specific doctrine.

C1.5 Reporting Responsibilities. The DISA Command Center (DCC) is the central control element for the Director, DISA. The DNCs which exercise operational direction over specified geographical areas and networks report to the DCC. Areas may be further reduced to geographic regions under the operational direction of FCOs, which have delegated responsibility for exercising

operational control over individual geographical areas or specific networks that report to the appropriate DNC. The TCFs are responsible for exercising operational control over subordinate PTFs and other GIG facilities and report to the appropriate FCO. The PTFs and other GIG facilities are responsible for reporting directly to the servicing TCF assigned within their specific geographic location. Although the DNCs may have remote monitoring and network management responsibilities for some GIG switching centers, the GIG switching centers are required to report specific requirements contained in this Circular and DISAC 310-55-1 (reference 4.1) through the designated TCF.

C1.6 Operating Messages. The DISA Operations Centers (i.e., DNCs) may issue messages or telephone instructions in exercising operational direction over GIG facilities.

C1.6.1 Operational Direction Message (ODM). An ODM directs actions or requests additional information involving the operational responsiveness of the GIG and normally requires direct, immediate actions by the GIG operating elements. An ODM is temporary. If long-term material is initially published by an ODM, the ODM will be canceled within 90 days, and its contents placed in official correspondence or directions. An ODM will be assigned and released only by the System Control Officer (SCO) or network controller on duty in the DISA Operations Centers. An ODM is numerically identified by the date-time group (e.g., 010001Z January 12). An ODM may be transmitted either by record message or by voice, depending upon the urgency of the situation; however, a voice ODM will be followed with a record copy within 24 hours. Appropriate instructions to GIG facilities will be initiated by commanders of DISA elements to ensure ODMs are distributed to appropriate personnel for immediate action. Information copies of an ODM will be sent to the appropriate O&M agencies and to higher and lateral elements of DISA.

C1.6.2 Operational Coordination Message (OCM). An OCM provides the capability for GIG facilities and subordinate DISA elements to respond to an ODM or to furnish nonaction information to higher or lateral elements. These messages will be identified in the same manner as an ODM. An OCM may be transmitted either by record message or by voice, depending on the urgency of the situation; however, a voice OCM is followed with a record copy within 24 hours. An information copy of an OCM is sent to other GIG facilities, O&M agencies, and DISA elements, as appropriate.

C1.6.3 Detailed Outage Report (DOR). A DOR may be requested by any DISA element to assist in the resolution of problems in the GIG. Reporting of communications failures and operational status from the lowest control level, via voice or record orderwires, to DISA elements is absolutely necessary. The purpose of a DOR is to provide immediate outage analysis information to higher level authorities. A DOR is normally requested when extenuating circumstances occur or during extensive outages on high interest circuits. A DOR is a nonformatted narrative type report that must be submitted as expeditiously as possible. Local requirements must not delay submissions. As a minimum, the FCO shift supervisor will provide a DOR to the appropriate DISA element within 2 hours of request with the following information: (1) a brief description of initial symptoms; (2) an analysis of troubleshooting efforts, test results, and any other pertinent information that occurred during the outage; (3) a clear reason for the outage, and, if the problem was not isolated to a definite problem, a "probable cause" will be listed; and (4) any recommendation(s) for improving service or how to prevent reoccurrence of this type problem (i.e., circuit routing, procedures used, etc.).

C1.7 Orderwires. Effective operation of GIG telecommunications facilities requires frequent coordination among technical controllers and maintenance personnel exercising technical control of the GIG. This coordination is accomplished over voice and data circuits between GIG and GIG elements used in disseminating operational direction over the GIG and in receiving GIG status reports.

C1.7.1 System orderwires are communications circuits or links, either voice or data, between selected nodal TCFs and FCOs. The functional point of contact (POC) has to evaluate and conduct global changes, if appropriate.

C1.7.2 Express orderwires are communications circuits, normally voice, between selected FCOs serving as Communications Control Office (CCO) or Intermediate Control Office (ICO) for a large number of trunks or circuits.

C1.7.3 Temporary orderwire circuits are communications circuits established as required by the FCO when available orderwires are not adequate for restoral of high priority circuitry or facilities. These orderwires may be voice or data, depending upon station capability. Normally, these temporary orderwires will be established as on call patches, as prescribed in chapter 5.

In the event that orderwires cannot be established by on call patch procedures due to preemption limitations imposed, the TCF will contact the appropriate FCO or DISA element for assistance. The functional POC has to evaluate and do global changes, if appropriate.

C1.7.4 Intercommunications circuits are communications circuits between the FCO and selected terminal locations within the DISN station complex at a specific geographic location.

Return to:

Basic Circular

Top of Table of Contents

DISA Publication Listing

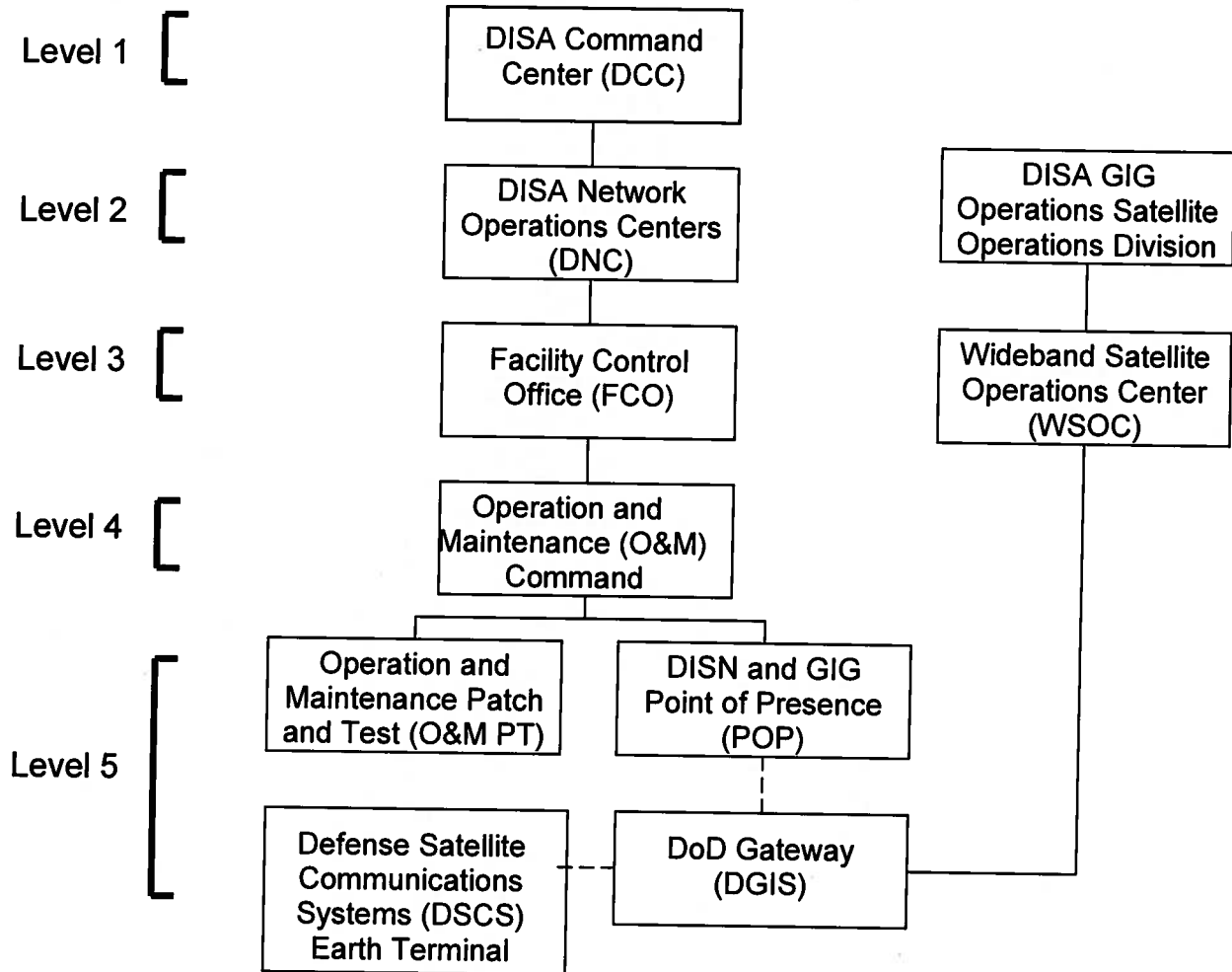
DISA Home Page

Continue to:

Chapter 2

DISA PUBS@DISA.MIL - Last change: 21 March 2012

FIGURE F1.1 GIG REPORTING HIERARCHY



Return to:

[Basic Circular](#)

[Top of Table of Contents](#)

[DISA Publication Listing](#)

[DISA Home Page](#)

Continue to:

[Chapter 2](#)

DISA PUBS@DISA.MIL - Last change: 21 March 2012

C2. CHAPTER 2. GIG CONTROL FACILITIES AND PERSONNEL

C2.1 **General.** This chapter defines the general configuration concept and criteria. It also details functions and duties of a Facility Control Office (FCO), Global Information Grid (GIG) Technical Control Facility (TCF), and GIG Patch and Test Facility (PTF) at levels 3, 4, and 5 of the DISA System control hierarchy. Levels 1 and 2 are at the DISA Command Center (DCC), DISA Network Centers (DNCs), and DISA operational levels for oversight on levels 3, 4, and 5. Operational control of maintenance support, technical controller skills and knowledge, facility qualification training, and familiarization and coordination visits are also addressed.

C2.2 **Configuration Concept and Criteria.** All GIG Technical Control Facilities (TCFs) and Patch and Test Facilities (PTFs) must be configured and engineered in accordance with the criteria of Military Standard (MIL-STD)-188-154A, Subsystem Equipment and Interface Standards for Common Long Haul and Tactical Telecommunications Control Facilities. Some of the basic concepts and criteria, detailed as follows, are designed to provide survivability, flexibility, standardization, and cost effectiveness of the GIG. Although non-GIG facilities are not required to meet the technical criteria of this Circular, they must attempt to provide the same technical characteristics for GIG circuits traversing their facility, especially when interfacing with GIG facilities. Non-GIG facilities meeting all the criteria of MIL-STD 188-154A may request identification as GIG facilities, in accordance with GIG facility definition in this Circular.

C2.2.1 GIG facilities must be configured and engineered to enable technical controllers, as well as other operations and maintenance (O&M) personnel, to maximize the full capabilities of the Defense Information System Network (DISN) equipment and personnel. These facilities must take into consideration the non-GIG tactical missions of the military departments (MILDEPs) and must be designed to achieve optimum standardization of equipment in terms of layout and procurement specifications, operating procedures, training, manning guidelines, and technical control functions. These facilities must be designed to enable the technical controller to effectively exercise assigned functions and duties.

C2.2.2 Each GIG TCF is required to perform the functions of technical control of the GIG. Several control facilities may exist at a geographical location (GEOLOC), but only one facility

will be designated as the servicing GIG TCF. Other GIG facilities having patch and test capabilities must be designated PTFs and must be technically compatible with the servicing GIG TCF. All GIG trunks and circuits must be routed through existing GIG TCFs or PTFs or be remotely monitored and controlled by another GIG facility or DISA Network Monitoring Center (MC) (e.g., Defense Switched Network [DSN] circuits not routed through a TCF which can be monitored and tested with a maintenance and administration facility terminal) or through DISA-approved commercial control facility. This includes all trunks and circuits government-owned or leased ordered by DISA Telecommunications Service Order (TSO) action. At those GEOLOCs without a GIG TCF or PTF and where remote monitoring and controlling capabilities do not exist, efforts must be made to ensure GIG trunks and circuits are routed through existing non-GIG facilities that have similar capabilities or through DISA approved commercial control facilities. The criteria outlined as follows must be adhered to as long as it is technically feasible, cost effective, and does not violate commercial tariffs.

C2.2.2.1 All transmission media and interface equipment must meet and be maintained in accordance with GIG performance standards. (Refer to DISAC 300-175-9, Global Information Grid (GIG) Operating-Maintenance Electrical Performance Standards (reference 4.4), and DISAC 310-130-2, Management Thresholds and Performance Objectives (reference 4.5)). Any portion of a system or circuit that fails to meet GIG performance standards must be corrected prior to acceptance. If the system or circuit is accepted with exceptions, the cause must be annotated and appropriate action taken to correct the exceptions or obtain a waiver from the appropriate DISA allocation and engineering (A&E) activity. This applies to all entities that perform testing on equipment and circuits that traverse the tech control and/or patch and test, (e.g., tech controllers, DISA, and Service government and contractor personnel). In the event the tech controller is not performing the testing, the personnel performing the testing will hand over appropriate documentation that validates the installation and implementation, in accordance with DISAC 300-175-9 (reference 4.4) and DISAC 310-130-2 (reference 4.5), to be added to the circuit history folder.

C2.2.2.2 All circuits and trunks, digital or analog, that traverse GIG TCF must be accessible for purposes of quality control testing, performance monitoring, operational control, rerouting, and restoral. PTFs must be designed with similar capabilities, although some capabilities may be limited.

C2.2.2.3 All user interfaces must be conditioned to meet GIG transmission standards. All circuits traversing the GIG TCF or PTF in analog form must be conditioned to provide equal transmitting and receiving levels, in accordance with MIL-STD-188-154A.

C2.2.2.4 The capability for manually patching or electronically switching spare equipment must be provided to permit timely equipment substitution and circuit conditioning. This includes the capability to provide at least ten percent additional conditioning, interfacing, and ancillary equipment for expansion, as required by MIL-STD-188-154A. GIG TCFs interfacing with long haul transmission media must be configured and equipped to provide at least one standby conditioning string for every ten strings (or portion thereof) of the same configuration.

C2.2.2.5 The orderwire networks remain an effective emergency means of communications between the DISA elements and O&M facilities supporting DISA levels 3, 4, and 5 functions.

C2.2.2.6 All unattended alarm indicators essential to performance of GIG network elements (NEs) should appear in the TCF or PTF for performance and alarm monitoring. This includes but is not limited to radio and multiplex alarms, major and minor alarms from GIG switching equipment (e.g., DSN, internet protocol [IP] router networks), power supply alarms, and timing and sync alarms (e.g., cesium beam and global positioning system [GPS]). An exception is for DISA-managed GIG systems monitored remotely by the servicing network operations centers.

C2.2.2.7 Each GIG TCF or PTF is required to have site specific systems diagrams that depict signal flow through the facility readily available in the operations area of the TCF or PTF to aid restoration and troubleshooting efforts. DISA network diagrams are not a part of this requirement; however, they may be solicited and approved at the discretion of the Theater Transmissions Office. At a minimum, these diagrams must include interface, multiplex, timing, and transmission equipment configurations that indicate the required frequencies, transmission level point (TLP), signal levels, and noise levels for analog transmission media. Digital transmission media must include bit rates, bit error rate specification, and timing and sync information.

C2.2.2.8 In-facility circuit layout records (CLRs) must be completed for all trunks and circuits that have a physical appearance in the TCF or PTF and for all trunks and circuits for which the TCF or PTF is the servicing TCF or PTF. The CLR must depict "in-facility" equipment and cross-connect information. The reverse side of a DD Form 1441: Circuit Data Card, which is used to identify circuits, links, and trunks, along with their restoral priority, may be used to satisfy this requirement. Other methods, including automated, may also be used. TCF or PTFs with numerous circuits of the same configuration (e.g., DSN interswitch trunk [IST]) may use one CLR that depicts the common configuration, as long as specific cross-connect, conditioning equipment, and other pertinent information is maintained for each individual circuit.

C2.2.2.9 CLRs for analog circuits must include audio signal levels, type signaling, and signaling frequency for each TLP.

C2.2.2.10 CLRs for digital circuits must include timing (e.g., synchronous, asynchronous, or isochronous) and configuration (i.e., equipment timing [external, internal, recovered, etc.]); any specialized configurations or strapping options that are required for the device to function properly; data rate; electrical and mechanical interface type (i.e., RS-232, RS-449, MIL-STD-188-114A, etc.); signal type (i.e., non-return-to-zero (NRZ), Bipolar/Alternate Mark Inversion (AMI), B8ZS, etc.); protocol (i.e., Bisync, high-level-data-link-control (HDLC), synchronous-data-link-control (SDLC), etc.).

C2.3 Functions and Duties of a Facility Control Office (FCO).
The FCO function is the tie between the tech controllers, patch and tests, all level 4 and 5 entities of the GIG Operations Hierarchy, and the DISA Network Operations Centers (DNCs). FCOs can be designated by service agency, such as the Army AGNOSC, Navy NAVGNOSC, Air Force AFNOSC, Marine MCNOSC, and other specific Global Network Operations Service Centers (GNOSCs) or Network Operations Service Centers (NOSCs). Subject to the specific theater or service agency, some FCOs are not aligned with a Service and may be aligned by area of responsibility (AOR), identified combatant commands, theaters, etc.; however, the purpose of the FCO remains unchanged. Personnel within a FCO should have, at a minimum, the same qualifications as the personnel in the communications facilities that they oversee. They should be trained on how the facilities support the combatant commands in order to sustain its mission and the understanding of where that area

fits into the theater communications systems. In addition, they should also be well versed in the Joint Concept of Operations and GIG NetOps construct. FCOs can also be assigned by region within a specific theater at the discretion of the combatant commands. FCOs may designate subordinate facilities as Intermediate Facility Control Offices (IFCOs), with the concurrence of the Service, to assist the FCO with the management and control of large geographical areas. When designated, IFCOs have the same basic functions as that of an FCO. FCOs must be manned 24 hours per day, have sufficient communications capabilities to coordinate with the appropriate DISA level 2 facility DNC, and be able to provide operational control over subordinate facilities. Each FCO must have at least one means of secure communications capability that is compatible with the DISA level 2 facility. FCOs respond to operational direction from level 2 of the GIG Systems Hierarchy, DISA Network Center (DNC), and mission critical situations and can also be directed from level 1 of the GIG Operation Hierarchy and DISA Command Center (DCC). The minimum functions and duties of an FCO are as follows:

C2.3.1 Exercise operational direction and management control over all assigned subordinate GIG facilities, transmission systems, and networks, etc., and perform network management functions as assigned by DISA.

C2.3.2 Function as the reporting facility for all assigned subordinate GIG facilities, transmission systems, networks, etc.

C2.3.3 Develop specific operating procedures pertinent to the area of assigned responsibility and distribute these procedures to all hierarchical elements and to subordinate facilities (e.g., DISA, DCC, DNC, IFCO, TCF, and PTF) having responsibility within that area and or as a service entity.

C2.3.4 Be the focal point for the GIG Station Reporting Guide and GIG Facility and Link Reports. (The FCO is to distribute these products to subordinate facilities and ensure subordinate facilities review and update the products. The FCO is to determine if updates will be forwarded back through the FCO or directly to the appropriate DISA element. When an IFCO is assigned, the FCO will distribute the products to the IFCO, and the IFCO is to distribute to their subordinate facilities. Reports for unmanned locations are to be forwarded to the next higher O&M command element.)

C2.3.5 Record and report all GIG outages and degradations occurring at subordinate facilities, in accordance with DISAC 310-55-1, Status Reporting (reference 4.1), and area supplements.

C2.3.6 Maintain a Master Station Log (MSL) to record information on significant events occurring within the area of assigned responsibility. (Facilities having dual responsibilities (i.e., FCO and TCF or PTF) can maintain one log as long as the FCO entries are properly identified.)

C2.3.7 Maintain situational awareness of the current operational status of all subordinate facilities including specific networks (e.g., IP router networks, DSN).

C2.3.8 Be the focal point for DISA area restoral plans (R-Plans), minimum essential circuit listings (MECLs), and local restoral plans (LRPs); assist in the development of the facility, coordinate periodic review with subordinate facilities, and ensure subordinate facilities provide corrections to DISA; and approve LRPs for subordinate facilities and maintain current copies of DISA R-Plans, MECLs, and LRPs.

C2.3.9 Direct subordinate facilities to implement restoral plans during major system failures to support exercises, etc., as directed by the DNC. (The FCO cannot implement DISA area R-Plans or MECLs without authority from the DNC. As the network install base increases, the need for R-Plans become less essential due to advanced communications systems automatic reroute capabilities. In the case where traffic is not automatically restored, R-Plans facilitate the rerouting of communications traffic, in accordance with Telecommunications Service Priorities (TSPs) and MECLs.)

C2.3.10 Maintain a listing of all major equipment installed at subordinate DISN facilities. (A current copy of each facility's GIG facility and link report is sufficient.)

C2.3.11 Request and direct special testing to isolate system and network problems.

C2.3.12 Refer system or network problems beyond the capability of the FCO to the DNC.

C2.3.13 Act as the sole approving authority for authorizing temporary removal of diversity equipment at subordinate DISN facilities. (Except for emergencies, diversity equipment must not be taken offline during peak traffic periods unless the FCO deems it absolutely necessary. Other disruptive maintenance actions, such as switching to standby equipment, are not authorized during peak traffic periods. Any of the above actions have the possibility of causing degradation to GIG systems, especially to timing and synchronization signals on digital systems that may affect numerous data circuits.)

C2.3.14 Coordinate authorized service interruptions in accordance with DISAC 310-55-1 (reference 4.1).

C2.3.15 Review performance data of subordinate sites, as determined by the DCC, to include Performance Monitoring Program (PMP) data, outage trend analysis data, etc.; assist in the resolution of problems identified; and refer problem with poor performance and repeated trend analysis failures to DISA operation centers for technical assistance.

C2.3.16 Host an annual meeting with subordinate facilities to address technical, managerial, and administrative issues that affect GIG operations.

C2.3.17 Maintain a DISA reference library, in accordance with chapter 9, and any applicable DISA DNC supplements. (If the facility has computers with network access to the military domain (.mil), it is acceptable to provide links with the DISA Web page for the most current versions of the Circulars effectively negating the need to maintain hard copies.)

C2.4 Functions and Duties of a GIG Technical Control Facility (TCF). The minimum functions and duties of a TCF are as follows:

C2.4.1 Respond to operational direction from the DCC and O&M control elements (e.g., FCO, AGNOSC, and AFNOSC).

C2.4.2 Exercise technical control, coordination, and supervision over subordinate GIG facilities, GIG transmission systems, trunks, and circuits. (Technical control extends to unmanned facilities that are under the control and supervision of a TCF.)

C2.4.3 Report the status of facilities, transmission links, trunks, and circuits, in accordance with DISA reporting

directives and submits status reports, in accordance with DISAC 310-55-1 (reference 4.1), DISA NetOps, and DISA DNC supplements.

C2.4.4 Coordinate and troubleshoot with DISA NetOps centers, adjacent facilities, customer agencies, maintenance organizations, and commercial vendors to troubleshoot, isolate, repair, and effect restoration of service.

C2.4.5 Implement DISA R-Plans, minimal essential circuit listings (MECLs), and local restoral plans (LRPs), as directed by the DISA element or FCO or Service NetOps component, and restore disrupted service to users that are not covered by R-Plans by using any other existing communications capabilities.

C2.4.6 Assist in the development of DISA R-Plans and MECLs, as requested; develop LRPs; perform periodic review of all R-Plans and ensure corrections are provided to the DISA element and to the appropriate FCO and Service NetOps component; and maintain current copies of these plans.

C2.4.7 Perform quality control tests and measurements on all applicable trunks, channels, circuits, and equipment for which the TCF is responsible.

C2.4.8 Ensure quality of GIG transmission, timing and synchronization, multiplex, and switching equipment using installed monitoring capabilities and appropriate communications test equipment.

C2.4.9 Review and analyze system, trunk, circuit, and equipment performance and coordinate and assist in troubleshooting, isolating, repairing, and correcting the unsatisfactory condition or fault, in cooperation with other facilities, customer agencies, maintenance organizations, commercial vendors, and DNCs.

C2.4.10 Perform testing and acceptance and activate, change, and deactivate trunks and circuits, in accordance with chapter 6 and DISA Telecommunications Service Orders, or as directed by higher levels of control (e.g., DNCs and DCC) in times of stress including tactical trunks and circuits and submit applicable reports (i.e., delayed service, exception, ineffect), in accordance with DISAC 310-130-1, Submission of Telecommunications Services Requests (reference 4.6).

C2.4.11 Perform network management functions, including bandwidth control, for those networks which responsibility has been assigned.

C2.4.12 Request authorized service interruption (ASI) for subordinate facilities from the appropriate DISA element, in accordance with DISAC-310-55-1 (reference 4.1) and control routine downtime for preventive maintenance and other actions requiring equipment substitution.

C2.4.13 Arrange for user release of individual circuits for out-of-service quality control testing, routine maintenance, and other scheduled service interruptions.

C2.4.14 Perform administration and record keeping functions required by DISA Circulars.

C2.4.15 Submit facility or link data, in accordance with DISA NetOps, DISA DNC supplements, or FCO instructions.

C2.4.16 Submit corrections to DISAC 310-55-1 (reference 4.1), DISA DNC supplements, or FCO instructions.

C2.4.17 Submit a DD Form 1368: Modified Use of Leased Communication Facilities, on leased circuit outages, when responsibility has been assigned, in accordance with DISAC 350-135-1 (reference 4.11) and DISAC 310-130-1, Submission of Telecommunications Service Requests (reference 4.6).

C2.4.18 Report meaconing, intrusion, jamming, and interference (MIJI) of electromagnetic systems, in accordance with Service directives on all affected GIG systems, with an information copy to the FCO and the DISA elements.

C2.4.19 Establish local written procedures for the following:

C2.4.19.1 Methods of coordination with the DISA, adjacent facilities, user agencies, maintenance agencies, and commercial vendors. (Procedures must include telephone numbers and any significant instructions.)

C2.4.19.2 Actions to be taken in the event of a contingency or significant communications failure to include reroute plans, reporting, and other procedures required to ensure continuity of service. (These instructions must contain actions to take in case of any natural [i.e., fire, flood, hurricane, etc.]

or hostile [i.e., terrorist attack, protests, etc.] event that is probable for that area. Instructions must include detailed actions for securing, transporting, or destroying classified material.)

C2.4.19.3 Actions to be taken in the event of primary and/or backup power failures, including procedures for load shedding. (Written procedures must be included for operation of backup power equipment if TCF or PTF personnel are required to perform such tasks.)

C2.4.19.4 Operation of site specific network management systems; such as, a transmission monitoring and control and matrix switches. (Procedures should include such actions as access policy and password control, actions to be taken when equipment alarms are received, procedures for backing up data [e.g., optical media and network drives], and actions to take if the data becomes corrupted.)

C2.4.20 Send GIG user notification memorandums to each user upon activation of a new circuit and annually thereafter. (An updated memorandum should also be sent any time information contained in the memorandum affects the user's ability to contact appropriate personnel [i.e., phone number, point of contact (POC), etc.]. [A sample of a GIG User Notification Memorandum is provided at figure F2.1. If used, the sample memorandum should be modified to include local requirements.]

C2.4.21 Label all patch bays, test boards, cabling, or other circuit access points normally used by technical control personnel. (As a minimum, labeling must include the last four characters of the circuit command communications service designator (CCSD) and the National Communications System (NCS) and Telecommunications Service Priority (TSP) restoration priority. If an NCS TSP is not assigned, then the letters "NA" (none assigned) must be entered with the CCSD to indicate the circuit has no assigned restoration priority.)

C2.4.22 Maintain a current DISA reference library readily accessible to the technical controllers. (A list of basic reference documents is contained in chapter 9. DISA areas may supplement this list, as necessary. If the facility has computers with network access to the military domain (.mil), it is acceptable to provide links the DISA Web page for the most current versions of the Circulars and negate the need to maintain hard copies.)

C2.4.23 Publish and post notices to technical controllers, including additions, deletions, or changes in circuitry and equipment; special missions being supported; special tests on circuits or equipment; changes in operational procedures; and any additional information considered appropriate.

C2.5 Functions and Duties of a GIG Patch and Test Facility (PTF). GIG PTF personnel have the same functions and duties as GIG TCF personnel with the exception that the physical and electrical capabilities of the GIG PTF may be limited.

C2.6 Additional Functions and Duties of TCF or PTFs.

In addition to the normal functions and duties, level 4 and 5 facilities may be designated control offices for the activation, change, or deactivation of GIG trunks and circuits and have primary responsibility for establishing and maintaining the end-to-end alignment and quality of assigned GIG trunks and circuits. These control activities focus on local equipment capabilities and user interface with the GIG. The three types of control offices are Communications Control Office (CCO), Intermediate Control Office (ICO), and Communications Management Office (CMO). A CCO or CMO must be assigned to every Defense Information System Network (DISN) trunk and circuit by the DISA allocation and engineering (A&E) activity and must be included in the Telecommunications Service Order (TSO). The CCO or CMO has primary responsibility for ensuring transmission facilities provide maximum quality service to users of the GIG. This requires testing and monitoring of parameters, threshold violations, alarm status, error rates, and other such indicators of transmission media performance.

C2.6.1 Communications Control Office (CCO).

C2.6.1.1 A CCO exercises direct technical supervision over assigned GIG trunks and circuits. A CCO must have the capability to test and monitor the trunk or circuit, ascertain that the trunk or circuit meets specified technical parameters, direct necessary adjustments, assess operational status, and perform other such functions required to establish and maintain high quality, user-to-user communications. These capabilities may be either manual or automated. All other facilities that the trunk or circuit traverses must respond to the technical direction of the CCO. The CCO initially activates the trunk or circuit, accepts leased service on behalf of the U.S. Government, and submits appropriate completion reports required by the TSO issuing authority.

The CCO coordinates all realignment, when necessary, to maintain the end-to-end engineered values stated in the TSO. CCO assignments must be made as follows: (1) when a trunk or circuit traverses a GIG TCF or PTF, a GIG TCF or PTF must be assigned as the CCO; (2) when a trunk or circuit does not traverse a GIG TCF or PTF, but does traverse another GIG facility that has testing and monitoring capabilities, then that GIG facility must be assigned as the CCO; (3) when a trunk or circuit does not traverse a GIG facility, but is remotely accessible by a GIG TCF or PTF or other GIG facility, then that TCF or PTF or facility must be designated as the CMO; and (4) when a circuit does not traverse a GIG facility, then a CMO must be assigned in accordance with subparagraph C2.6.3. Specific CCO duties include the following:

C2.6.1.1 Coordinate the activation, deactivation, and change of trunks and circuits with applicable facilities, users, DISA DNCs, and commercial vendors.

C2.6.1.2 Immediately, upon receipt of a TSO, coordinate with each facility, user, DISA DNC, and commercial vendor involved, to ensure all parties are capable and ready to provide the required service.

C2.6.1.3 Ensure the completion of all initial quality control tests, direct necessary adjustments, and ascertain that the trunk or circuit meets the specified technical schedule before acceptance.

C2.6.1.4 Prepare and submit completion reports for which control responsibility has been assigned.

C2.6.1.5 Immediately advise the TSO issuing authority and all other addressees on the original TSO of any conditions which might affect service activation. (Such conditions would include failure to meet TSO specifications, nonavailability of leased circuit segments, etc.) Ensure service reports (i.e., delay, exception, or ineffect) are submitted in accordance with DISAC 310-130-1 (reference 4.6).

C2.6.1.6 Provide technical assistance to other facilities, users, and commercial vendors when they are unable to isolate degradation(s).

C2.6.1.7 Immediately report all instances of unsatisfactory response from other facilities, users, or commercial vendors to the FCO, requirement approval authority, or DISA, whichever is appropriate.

C2.6.1.8 Establish local procedures for receiving, monitoring, and completing trunk and circuit TSO actions.

C2.6.1.9 Develop and distribute quality control test schedules with applicable facilities, users, and commercial vendors.

C2.6.1.10 Document, analyze, and maintain quality control test data, as required by this Circular.

C2.6.1.11 Conduct trend analysis on performance of assigned trunks and circuits, in accordance with chapter 6.

C2.6.2 Intermediate Control Office (ICO). If the layout of a circuit or trunk is such that the CCO is not in the best position to test or coordinate activities with intermediate facilities, another facility may be designated as an ICO to assist the responsible CCO. ICO assignments are normally only made on circuits traversing long distances (e.g., one DISA TNC to another). ICOs must be designated in the segment portion of the TSO. Temporary ICOs may be designated by the appropriate TSO issuing authority for the specific purpose of completing TSO change actions. ICOs report to the CCO for operational direction.

C2.6.3 Communications Management Office (CMO). A CMO is a facility or office that is assigned administrative responsibility for GIG trunks and circuits when it is not possible to assign a GIG facility as the CCO. The CMO serves as the focal point for day-to-day monitoring of service performance, accepts service on behalf of the U.S. Government, and submits applicable reports in accordance with DISAC 310-130-1 (reference 4.6). The CMO is responsible for the same basic functions as a CCO with the exception of actual monitoring, testing, and troubleshooting. If any form of monitoring and testing capabilities does exist, the CMO must make every effort to assist when necessary. CMO assignments must be made in accordance with the following guidelines: (1) when the trunk or circuit traverses, or is monitored by a non-GIG facility operated by a MILDEP O&M that has capabilities similar to a CCO, then the non-GIG facility should be designated as the CMO, (2) when a CCO cannot be assigned to a IP router network

circuit, the Node Site Coordinator (NSC) should be assigned as the CMO, and (3) when a trunk or circuit does not traverse and cannot be monitored by a GIG or non-GIG facility, then some office or activity associated with the using agency of the trunk or circuit should be assigned CMO.

C2.7 Operational Control of Maintenance Support. The complex nature of the GIG requires extensive coordination between the TCF or PTF and maintenance support elements to achieve maximum efficiency of transmission systems. The TCF or PTF must maintain operational control over all equipment supporting the GIG operations at all times and will have final authority for determining the operational acceptance of all equipment after maintenance, alignment, or repair; approval of online maintenance; and approval to remove operational equipment from service. The TCF or PTF is responsible for the following actions:

C2.7.1 Determining the priority of maintenance on all equipment supporting GIG operations.

C2.7.2 Ensuring corrective maintenance is performed in the order dictated by the Department of Homeland Security (DHS) and Telecommunication Service Priority (TSP) system of the trunks or circuits that are degraded.

C2.7.3 Ensuring maintenance schedules are coordinated with the TCF or PTF and that TCF or PTF personnel are aware of maintenance actions affecting GIG operations.

C2.7.4 Coordinating maintenance actions with other GIG facilities when those facilities are affected.

C2.7.5 Performing appropriate quality control tests when equipment is returned from maintenance, before putting it back into operation.

C2.7.6 Ensuring maintenance technicians obtain approval from the TCF or PTF shift supervisor before any equipment in support of the GIG is taken offline for maintenance or before any online maintenance is performed. (Diversity equipment is not authorized to be taken offline, nor is any type of disruptive maintenance action allowed, during peak traffic hours without approval of the FCO. Peak traffic hours are established by each DISA DNC.)

C2.7.7 Ensuring strapping, pinning, and programming options on installed GIG equipment and cards is documented and available. (Maintenance activities will normally have this information; however, if TCF or PTF personnel are responsible for replacing cards, they must have the necessary information available to ensure the cards are properly configured if replacement becomes necessary. This information is especially critical for time division multiplexed (TDM) and data transmission equipment that have specific protocols and interfaces.)

C2.8 Technical Controller Skills and Knowledge. Technical control personnel must know, understand, and be able to apply the following concepts, theories, and tasks. This list is not all inclusive and must be supplemented according to local requirements.

C2.8.1 Basic telecommunications principles, protocols (7-layer open system interconnection [OSI] model), terminology, and concepts.

C2.8.2 Electrical and electronic fundamentals to include theory and operation of solid state devices and other circuit elements of communications equipment.

C2.8.3 Principles, theory, and characteristics of transmission media including microwave, satellite, tropospheric scatter, high frequency (HF), and metallic and fiber optic cables.

C2.8.4 HF radio communications systems propagation charts, forecast data, and sounding techniques.

C2.8.5 Principles and application of analog (e.g., channel, group, supergroup) and digital (e.g., DS-0, DS-1, DS-3, OC3, STM-1) multiplex equipment and transmission media and be able to test signals through the local multiplex equipment and determine if signals meet specifications.)

C2.8.6 Principles and applications of Local Area Networks (LANs), Wide Area Networks (WANs), Fiber Distributed Data Interface (FDDI), Integrated Services Digital Network (ISDN), and packet switching.

C2.8.7 Principles and applications of digital timing and synchronization.

C2.8.8 Operate a personal computer and use operating system commands and application software programs; such as, database management systems, word processing, graphics, etc.

C2.8.9 Have a basic understanding of internet protocol (IP), Layer 3 in OSI Model, addressing and packet routing.

C2.8.10 Be able to use local onsite computer terminal(s) for administrative or network specific functions; such as, transmission monitoring control, network management, circuit implementation, troubleshooting, etc.

C2.8.11 Fundamentals of transmission monitoring and control terminal equipment.

C2.8.12 Common noise power measurements (e.g. dB, dBm, dBm0, dBmC, dBmC0, dBr, dBrn, dBrn0, dBrnC0, dBW) and be able to convert from one to another.

C2.8.13 Function and application of electronic hand tools.

C2.8.14 Ability to explain how to diagnose, remove, and replace circuit boards; such as, TDM cards, amplifiers, pads, equalizers, bridges, channel cards, etc.

C2.8.15 Principles and applications of various types of test devices, such as dB/volt/amp meters, oscilloscopes, signal generators, frequency counters, noise meters, delay equalizers, impulse noise sets, bit error rate tests (BERTs), protocol analyzers, distortion analyzers, etc., and be able to interpret measurement data.

C2.8.16 Principles and application of conditioning and signaling equipment.

C2.8.17 Patch panel and cross-connect (manual and electronic) principles.

C2.8.18 GIG connectivity and available reroutes associated with the local facility and proficiency at rerouting trunks and circuits.

C2.8.19 Ability to read and interpret equipment and patch panel schematic diagrams and circuit layout records.

C2.8.20 Isolate causes of interference and recognize various types of circuit troubles.

C2.8.21 Determine communications capabilities and be able to communicate with connected facilities.

C2.8.22 Understand and follow procedures and requirements for submission of GIG reports.

C2.8.23 Perform quality control test measurements and analyze results.

C2.8.24 Initiate and/or assist user to facilitate Telecommunication Requests (TRs) and act upon Telecommunications Service Orders (TSOs).

C2.8.25 Knowledgeable of MILDEP supply procedures.

C2.9 Facility Qualification Training. The training required of all new site technicians to acquire pertinent site specific knowledge, as well as sustainment training for the more experienced personnel, is detailed as follows:

C2.9.1 Site and sections training that consists of site certification, sustainment training, and special duty training is to be established by all site supervisors and team leaders. Examples of training required for an operator during their first 6 months in a TCF are as follows:

C2.9.1.1 Site certification training should identify specific training tasks which all personnel are required to master within specified time periods after arriving on station. All sites and sections must develop training following the same guidelines to those items listed below for site certification training. It is recommended that, at a minimum, TCF sites train and certify new personnel on the following:

C2.9.1.1.1 Newly arriving personnel should be trained on the following during their first month of duty:

- DISA, DISN, and O&M facility management hierarchy
- DISACs and publications (familiarity)
- Reporting requirements (DISAC 310-55-1 and O&M specific)
- Hazardous conditions (HAZCONS)
- Station power subsystems
- Environmental control systems air conditioning (AC) and heating
- Orderwire procedures
- Standard Operating Procedures (SOPs)
- Master Station Logs (MSLs)

- Outage and Restoration Record
- Circuit Data Cards
- Basic patching concepts and signal flow
- Daily walk-through checks
- Station grounding system
- Shift change procedures
- Facility's transmission connectivity

C2.9.1.1.2 By the third month, newly arriving personnel should be trained and certified on the following:

- Basic troubleshooting procedures
- Operation of test equipment
- In and out of service quality controls
- Conducting preventative maintenance
- Restoral plans (R-Plans)
- Authorized service interruption (ASI) procedures

C2.9.1.1.3 By the sixth month, newly arriving personnel should be trained and certified on the following:

- Master station timing system O&M
- Scheduling maintenance
- Operation, maintenance, and troubleshooting of multiplexers and modems
- Circuit activations and TSOs
- Trend analysis

The areas listed above are not all inclusive and should be used as a general guideline to assist site managers. The training plan should be adapted to include all equipment and duties within the facilities operational duties. Tasks may be added, and the timeline may be made more stringent; however, it is highly recommended that this timeline not be reduced. These timelines should be progressive. Tasks that are more complex and require certification by the third or sixth month should be taught in phases to build personnel proficiency in accordance to their skill level. By building the training up in phases, the individual will retain more of the subject matter each time the subject training is expanded to be more indepth.

C2.9.1.2 Sustainment training should be developed in a perpetual training schedule that identifies requirements and timeframes for all personnel on critical tasks and tasks that are not common functions which would require familiarization training to remain proficient. The schedule should be a long-range plan covering at least 1 calendar year.

C2.9.1.3 A special duty training plan should be created which outlines tasks required for site supervisor, maintenance and supply supervisor, circuit activations manager, node site coordinator, and shift supervisors certification. Each plan should be tailored to that position's specific functions and duties.

C2.9.2 Training outlines should be created for each subject specified in all of the training plans. These outlines should identify and provide safety considerations, as well as a detailed training assessment method consisting of a written test and hands on evaluation which specifies the exact requirements for achieving certification. The instructor of the task will not evaluate the trainee. A third person qualified to instruct the task will perform the evaluation in order to maintain consistent high training standards.

C2.9.3 A training manager will be assigned to oversee the training program. The training manager is to assign qualified individuals to be trainers; ensure all trainees meet training milestones; ensure training and certification standards are kept to the highest standards possible; maintain training records; process, verify, and issue certifications; and evaluate mission requirements and recommend schools, courses, or classes necessary to maintain mission readiness

C2.9.4 An individual training record shall be maintained on each individual assigned to the facility. The record should consist a listing of subjects and subtasks for which the individual is required to be certified, the date(s) training was conducted along with the trainer's initials, and the date certification was received with the certifier's initials.

C2.10 Familiarization and Coordination Visits. All assigned technical controllers should make familiarization visits to connected facilities, remote transmitter and receiver sites, radio relay sites, and high volume users that are colocated with the GIG station. Ideally, this would be part of an individual's facility qualification requirements. The TCF chief and other members of the TCF staff must make an effort to visit each major user and adjacent GIG facilities at least annually. The objective of these visits is to achieve good operating relationships between personnel of each facility and an understanding of the other facility's capabilities and problems. These visits can often be made when operational requirements dictate the need for a visit.

C2.11 **Duties of GIG Users.** Just as the servicing TCF and PTF has a responsibility to each user, each user has a responsibility to the servicing TCF or PTF. (Basic duties are outlined in a GIG User Notification Memorandum. [An example of the memorandum is provided in figure F2.1.]) All users of the GIG must cooperate with their servicing TCF or PTF to ensure high quality and reliable service. The servicing TCF or PTF is the critical interface point between the user terminal and the DISN transmission media. Restoration of service during degradations may be delayed if sufficient coordination and information is not provided. Specific duties include the following:

C2.11.1 Immediately reporting service interruptions directly to the servicing TCF or PTF.

C2.11.2 Providing continual coordination with the servicing TCF or PTF until service has been restored and accepted by the user.

C2.11.3 Cooperating with the servicing TCF or PTF in the performance of circuit quality checks. (A circuit is not considered restored until service is extended from user terminal to user terminal and circuit conditioning meet the standards prescribed in DISAC 300-175-9 (reference 4.4). Where facilities cannot meet prescribed standards due to inherent or design characteristics, the circuit shall be brought up to the best obtainable quality and, in any case, must be capable of providing the required service.)

C2.11.4 Coordinating with GIG TCF or PTF personnel prior to performing any equipment changes, maintenance, troubleshooting, or any other actions that may affect the quality or continuity of service.

C2.11.5 Contacting the distant end user when requested to release a circuit(s) for a scheduled downtime and obtaining their concurrence.

C2.11.6 Obtaining concurrence from higher headquarters for circuit releases, when necessary.

C2.11.7 Releasing the circuit(s) to the servicing TCF or PTF.

C2.11.8 Initiating a Telecommunications Request (TR) via DISA Direct Order Entry (DDOE) with required official role for submittal and vented through appropriate release authority prior to making any equipment or configuration change(s) to service. (This includes changing terminal equipment, transmission speed, user location, etc. If approved, DISA will issue a Telecommunications Service Order (TSO) authorizing the change(s).)

Return to:

Chapter 1

Basic Circular

Top of Table of Contents

DISA Publication Listing

DISA Home Page

Continue to:

Chapter 4

DISA Pubs@DISA.MIL - Last change: 21 March 2012

Figure F2.1 **SAMPLE GIG USER NOTIFICATION MEMORANDUM**

(Prepared on Letterhead)

AFSK-EB-STCG

(Date Signed)

MEMORANDUM FOR GLOBAL INFORMATION GRID (GIG) SUBSCRIBER

SUBJECT: Responsibilities of a Global Information Grid (GIG) Subscriber

1. You have been identified as a subscriber of the GIG. Your Circuit Identifier is _____. This number is to be clearly marked on the terminal equipment, along with the telephone numbers listed below. The Technical Control Facility (TCF) is to operate, maintain, and troubleshoot the communications under the control of Seoul TCF facility. As a GIG subscriber, you are to report all circuit problems and outages (loss of service) to the Seoul TCF trouble desk, in accordance with DISA Circular (DISAC) 310-70-1, Global Information Grid (GIG) Technical Control. Your assistance will be required during troubleshooting to help quickly isolate the fault and rectify the problem. This will allow the TCF to provide the quality of service required. A complete list of our telephone numbers and e-mail addresses are provided as follows:

Trouble Desk: phone numbers
NCOIC/Site Chief: phone number and e-mail address
Yongsan Microwave: phone numbers
Korean Technician Supervisor/Circuit Actions: phone number
E-mail - e-mail address
Quality Control (QC) Coordinator: phone number
Email - e-mail address
FAX: FAX number

2. Our mission is to provide the highest possible quality communications service. Seoul TCF is staffed with at least one U.S. Army Soldier/Technician and one Korean Technician 24 hours a day, 7 days a week. During normal duty hours, we have six personnel onsite to assist. DISA defines a "circuit" as the complete communications path and user equipment. A circuit is both end user's terminating equipment, modems, cryptographic equipment, post cable system, and the long haul carrier system. If a circuit fault cannot be corrected within 10 minutes of the user's log out time, we are required by DISAC 310-70-1 to open an outage record to track the troubleshooting efforts made to correct the fault and report this information up the DISA chain of command. The outage records are maintained onsite for historical trend analysis for 1 year.

AFSK-EB-STCG Memo, Responsibilities of a Global Information Grid (GIG) Subscriber,
(Date Signed)

3. Although we are not responsible for the repair of your equipment or the post cable system, we are your first point of contact for circuit problems. Upon receiving a call from you, the subscriber, we will begin fault isolation procedures and coordinate with the appropriate agencies to make repairs. We are responsible for the GIG communication systems supporting the region, consisting of state-of-the-art fiber optic systems, digital microwave radios, and commercial networks.

4. Contact us anytime for circuit outage updates or any information that you may need pertaining to your circuit. Should there be any problems or if you are dissatisfied with the service provided, you may call or e-mail either me or my staff. We are available to assist and resolve issues in a timely manner.

5. The point of contact is (name) at (phone number) or (e-mail address).

Site Chief
SSG, USA
NCOIC, Seoul Tech Control Facility

Return to:

Chapter 1

Basic Circular

Top of Table of Contents

DISA Publication Listing

DISA Home Page

Continue to:

Chapter 4

DISA PUBS@DISA.MIL - Last change: 21 March 2012

C4. CHAPTER 4. GIG TRANSMISSION NETWORKS

C4.1 **General.** This chapter clarifies the overall view of the Global Information Grid (GIG) transmission networks. The GIG terrestrial transmission networks are a hybrid digital multiplexing system, asynchronous transfer mode (ATM) system, internet protocol (IP) carrier routers and switches, and optical carrier system technologies that will continue to evolve. These networks are fully automated to provide a seamless worldwide network grid to provide robust and reliable communications to the Department of Defense (DoD). The networks are monitored 24x7 at each of the DISA Network Operations Centers (DNCs). DISA program managers ensure overall procedures are developed when DISA programs are fielded. Depending on the complexity of the system and or network, GIG facilities may be required to supplement the overall procedures for exercising lower level control. In most cases, the Technical Control Facilities (TCFs) have little to no view into these networks. For facilities which have their own network elements to manage, the operations and maintenance (O&M) division must ensure those networks continue to operate and meet the technical specifications identified in DISAC 300-175-9, Global Information Grid (GIG) Operating-Maintenance Electrical Performance Standards (reference 4.4).

C4.2 **Bulk Encryption.** The purpose of bulk encryption of GIG links and trunks is to protect, during transmission, classified and unclassified information that is related to national security. Bulk encryption of GIG transmission links is required in accordance with DoD Directives. Bulk encryption must be included as part of each military department's (MILDEP) O&M operations security (OPSEC), communications security (COMSEC), and inspection programs for those GIG facilities that are responsible for providing bulk encryption. Restored procedures will be reviewed during DISA performance evaluations (PEs) to comply with these requirements. If a bulk encryption device fails, immediate action must be taken to restore service to all circuits traversing that link. Restoral can be accomplished in three ways: (1) switching to spare encryption devices when available, (2) rerouting circuits in accordance with DNC or local restoral plans to a system with active bulk encryption, and (3) rerouting links and trunks in accordance with DNC or local restoral plans to a system with active bulk encryption. Most importantly, DISA restoral plans must be initiated by the DNC or

DISA Command Center (DCC) to ensure all high visibility trunks, links, and circuit outages, as well as restorals, are properly reported.

C4.2.1 In accordance with national security policy, when temporarily bypassing the encryption device, certain transmission systems are prohibited from operating without bulk encryption. A listing of these systems will be maintained by each DNC and the list distributed to appropriate Facilities Control Offices (FCOs), Technical Control Facilities (TCFs), and Patch and Test Facilities (PTFs). Bulk encryption bypasses should not be performed unless it is verified that the bulk encryption device is defective. Bypassing bulk encryption devices on a GIG link or trunk is authorized only for the minimum time required to isolate and replace or repair a defective component in the system. As soon as the bulk encryption device is operable, the bypass must be removed.

C4.2.2 All bypasses of bulk encryption devices on government owned or leased links or trunks must be reported to the FCO, as soon as practical. The FCO must determine if any further action is necessary, to include notifying the appropriate DNC. If it is anticipated that the bypass will be necessary for an extended amount of time (i.e., parts on order, etc.), rerouting of sensitive circuits to a protected path should be highly considered. The TCF or PTF implementing the bypass must notify the FCO upon restoral of the bulk encryption device. The DNC or FCO may, at their discretion, require immediate reporting of bulk encryption bypasses. This action is normally required when critical missions or increased tensions occur within a specific theater.

Return to:

Chapter 2

Basic Circular

Top of Table of Contents

DISA Publication Listing

DISA Home Page

Continue to:

Chapter 5

DISA PUBLS@DISA.MIL - Last change: 21 March 2012

C5. CHAPTER 5. CONTINGENCY OPERATIONS

C5.1 **General.** This chapter details procedures necessary to provide maximum communications during contingency conditions. Continuity of communications service is the primary mission of the Technical Control Facilities (TCFs) and Patch and Test Facilities (PTFs) under stressed conditions. The reliability and survivability of the Global Information Grid (GIG) depends to a great degree on the skill and knowledge of technical control personnel. Contingency operations must be planned to maximize effectiveness in maintaining service continuity for as many users as possible. Preplanned actions that permit personnel to practice and develop skills and knowledge required to achieve efficiency under adverse conditions are as follows: each TCF must have documented plans available that provide precise actions to take during contingency situations, authority must be delegated to the TCF shift supervisor to implement contingency plans when conditions require such action, personnel must be capable of implementing contingency plans, and practical exercises must be conducted periodically to ensure efficiency. Under no conditions should user traffic be interrupted during exercises.

C5.2 **Telecommunications Service Priority (TSP).**

C5.2.1 The TSP system ensures priority treatment of our Nation's critical telecommunications services. TSP assignments are obtained from the Department of Homeland Security (DHS). Only those telecommunications services that meet DHS criteria are eligible for TSP assignments. (Refer to DISAC 310-130-4, Defense User's Guide to the Telecommunications Service Priority (TSP) System (reference 4.7), for details.)

C5.2.2 The DHS TSP system assigns a provisioning and or restoration priority level. Provisioning level assignments are identified in position 11 of the TSP authorization code. Restoration priority level assignments are identified in position 12 of the TSP authorization code. TSP restoration priority levels are 1, 2, 3, 4, and 5 with 1 being the highest priority. It is possible that a TSP assignment can be made for provisioning purposes but have no restoration priority level assigned, in which case a "0" will appear in position 12 of the TSP authorization code. If a circuit or trunk does not qualify for TSP provisioning or restoration, a TSP authorization code is not assigned. Refer to figure F5.1 for an explanation of the TSP identification code.

C5.3 Minimum Essential Circuit List (MECL). An MECL is used by the combatant commanders in the overseas theaters to assign certain priority circuit requirements during stressed conditions. MECLs are controlled by the combatant commanders and are implemented by the DISA Network Operation Centers (DNCs) by direction of the DISA Command Center (DCC). Only government owned GIG circuits within a combatant commander's area of responsibility (AOR) may be included on an MECL. An MECL cannot be enforced on commercially provided leased service. Each MECL must be submitted to the DHS TSP Program Office for TSP assignment, in accordance with DISAC 310-130-4 (reference 4.7). Once DHS assigns a TSP restoration priority level for MECL purposes, the combatant commander may assign subpriorities to determine an order of precedence by which services or circuits of equal TSP level should be restored during stressed conditions. Subpriority assignment is not authorized by any Service or Agency below the combatant command level. A DNC must maintain a copy of the approved MECL and distribute it to operation and maintenance (O&M) commands, Facility Control Offices (FCOs), and appropriate GIG facilities. Each DNC must provide guidance regarding distribution and implementation of MECLs to the GIG facilities responsible for implementing MECLs.

C5.4 On-call Service. On-call service provides a temporary path, using existing circuitry, between authorized users to fulfill unanticipated or special communications requirements. On-call service is not intended as a substitute to meet known communications requirements and normally should not be activated for a period exceeding 7 days. If it is known that service will be required for more than 7 days, the requesting activity should submit an emergency Telecommunications Request (TR), in accordance with DISAC 310-130-1, Submission of Telecommunications Service Requests (reference 4.6), or contact the appropriate DISA element and obtain approval for extended service.

C5.4.1 On-call service procedures are outlined as follows:

C5.4.1.1 Requests for on-call service should be placed through the appropriate DISA element within the theater where service is required. (In certain instances, when time does not allow coordination through the DISA element, the requesting activity may coordinate directly with the local communications element.)

C5.4.1.2 Upon receipt of a request for assistance, the appropriate DISA element must determine the type of service required. (Information that must be obtained from the

requestor is as follows: priority of the on-call request, in accordance with the National Communications System (NCS) TSP priority systems; originator of the request and addressee desired; type of service required (e.g., voice, data, etc.); type of signal (e.g., required levels for voice, data rate, etc.); type of security equipment required, if applicable; time the on-call service is required; and estimated duration of the on-call service. If voice service is requested, the level of precedence, in accordance with the NCS Voice Precedence System, must be determined.)

C5.4.1.3 Once the type of service is determined, the DISA element must determine the route to be used and notify GIG facilities that are required to provide the requested service and or assistance.

C5.4.1.3.1 If required, coordination will be effected with other DISA elements. In determining the route, consideration must always be given to selection of the most direct route available. Establishment of path must be accomplished by an analysis of available GIG circuits, irrespective of military department affiliation.

C5.4.1.3.2 Each GIG TCF must ensure all requests for on-call service are acted upon immediately. (Authority and priority of the service can be verified with the appropriate DISA element, if necessary.)

C5.4.1.3.3 When requested in advance, the TCF must make appropriate connections, conduct tests, and notify the user at least 15 minutes prior to the scheduled activation time.

C5.4.1.3.4 Normally, on-call service will be provided by utilizing spare capacity or circuits specifically allocated for on-call purposes. When spare capacity or circuits are not available, circuits with lower restoration priorities may be preempted for this purpose. When the on-call service cannot be established within the means available to the TCF, the TCF should contact the DNC.

C5.4.1.3.5 If the user reports circuit trouble, prompt action must be taken to clear the trouble or provide an alternate circuit, in accordance with normal restoration priorities.

C5.4.1.3.6 When notified by the user that the on-call service is no longer required, the TCF must coordinate with the distant end to break down any special circuit arrangements used and

restore the circuit path to its normal function. The TCF must notify the appropriate DISA element when on-call service is terminated.

C5.4.2 On-call services with validated NCS TSP priorities have preemption authority over circuits with lower priorities. Prior to preemption of any existing user circuit for on-call service, the user must be notified of the impending action. Immediately upon termination of the on-call service, coordination between the affected TCFs must be accomplished and the preempted circuit restored to service.

C5.4.3 The category of NCS Voice Precedence System must be verified and programmed into the switch software, whenever on-call service requires connectivity into GIG voice switching systems. The voice precedence category must be verified by the appropriate DISA elements. The DISA elements will then program the proper precedence category (if remote capability exists) or direct O&M switch personnel to program the precedence category. The NCS Voice Precedence System categories are as follows:

C5.4.3.1 FLASH is generally reserved for command and control (C2) of military forces essential to defense and retaliation; critical intelligence essential to national survival; conduct of diplomatic negotiations critical to the arresting or limiting of hostilities; dissemination of critical civil alert information essential to national survival; continuity of Federal Government functions essential to national survival; fulfillment of critical United States internal security functions essential to national survival; and catastrophic events of national or international significance. FLASH has precedence over any other type of on-call voice service having an immediate, priority, or routine precedence.

C5.4.3.2 IMMEDIATE precedence is reserved generally for situations which gravely affect the security of national and Allied forces; reconstitution of forces in a post-attack period; intelligence essential to national security; conduct of diplomatic negotiations to reduce or limit the threat of war; implementation of Federal Government actions essential to national survival; situations which gravely affect the internal security of the United States; civil defense actions concerning direction of our population and their survival; and before disasters or events of extensive seriousness having an immediate and detrimental effect on the welfare of the population. IMMEDIATE has precedence over priority and routine.

C5.4.3.3 PRIORITY precedence is reserved generally for expeditious action requirements by the originator and for furnishing essential information for the conduct of government operations. PRIORITY has precedence over any other type of on-call voice service having a routine precedence.

C5.4.3.4 ROUTINE designation applies to those official government communications which require rapid transmission but do not require preferential handling. Routine has no precedence over any other type of on-call voice service.

C5.4.4 On-call service will be reported in accordance with instructions contained in DISAC 310-55-1, Status Reporting (reference 4.1), when required by DISA. For reporting purposes, temporary command communications service designators (CCSDs) will be assigned by the appropriate DISA element.

C5.4.5 The Master Station Log (MSL) must be used to record all activity associated with the initial on-call service request, activation, and subsequent deactivation. A DD Form 1443: Outage and Restoration Record, must be completed to record activation, outage, and deactivation information pertaining to the on-call service for the entire period of activation.

C5.5 Tactical Circuits. The capability now exists for rapidly interfacing tactical communications equipment with the GIG. Many TCF and PTFs have permanently installed facilities to provide this capability. It is also possible for a tactical facility to interface with the GIG and then be designated as a GIG facility. As such, it is important for GIG TCFs and PTFs to provide assistance and direction to personnel of tactical units when interfacing with the GIG.

C5.5.1 Common roles and duties of tactical and GIG technical controls are as follows:

C5.5.1.1 An orderwire or equivalent voice communications between the tactical van and GIG TCFs and PTFs is crucial and will be established immediately, as coordination between the tactical van equipment operators is of utmost importance.

C5.5.1.2 The TCF and PTF supervisor and the tactical team chief must perform all connections of signal and grounding cables at the tactical interface box (TIB), in addition to discussing transmission level point (TLP) differences. All circuit levels must be engineered or conditioned to GIG specifications when interfaced with the GIG.

C5.5.1.3 The tactical equipment operator should follow normal lineup procedures while aligning the tactical radio and carrier equipment. The team chief, after satisfied the equipment is prepared to accept traffic, must coordinate with the TCF and or PTF to turn the system over for GIG acceptance testing. The TCF and or PTF personnel must check continuity and verify system and channel integrity between the GIG facility and tactical equipment.

C5.5.1.4 After determining the TLP interface requirements for voice frequency (VF) circuitry of the tactical carrier, TCF and or PTF personnel must adjust pads and amplifiers to satisfy the GIG TLP requirements (zero dBm at the equal level patch) and the tactical carrier inputs and outputs channel requirements.

C5.5.1.5 The TCF and or PTF must transmit a -10 dBm0 test tone at 1004 Hz over each VF circuit and coordinate with the tactical van carrier operators to have them adjust the channel gain for each channel at both carrier terminals to meet the prescribed level, in accordance with the appropriate Telecommunications Service Order (TSO).

C5.5.1.6 Once the tactical system has been turned over to the TCF and PTF for operational traffic, the tactical van carrier operator must coordinate with TCF and or PTF personnel prior to performing any equipment changes, maintenance, system troubleshooting or any other steps which may affect the quality or continuity of the systems and circuits.

C5.5.2 Tactical equipment operators are to accomplish the following:

C5.5.2.1 Test all external hookup cables and cable pairs. (TCF and or PTF personnel must be notified of any transposed, grounded, or otherwise bad pairs which will affect circuit termination.)

C5.5.2.2 Establish the tactical system and aligning the carrier equipment.

C5.5.2.3 Work closely with TCF and PTF personnel until all systems and circuits have been aligned, patched through, and are passing traffic.

C5.5.2.4 Inform the TCF and PTF immediately if any changes occur in system and circuit status.

C5.5.2.5 Ensure all tactical equipment is properly grounded. (Grounding should be made to the GIG facility ground to prevent separate ground loops.)

C5.5.2.6 Ensure all power is properly connected. (If GIG facility power is required, it must be coordinated, preferably prior to arrival, with respective GIG facility personnel.)

C5.5.3 TCFs and PTFs are to accomplish the following:

C5.5.3.1 Ensure cable or wiring connections to include ground hookups are securely fastened at the site tactical interface box.

C5.5.3.2 Assist the tactical personnel with connecting their cables into the tactical interface box.

C5.5.3.3 Condition circuits once channels are accepted from the tactical van equipment operator.

C5.5.3.4 Report all system and circuit activation and outages, in accordance with current relevant DISA Circulars and Instructions.

C5.5.3.5 Contact and coordinate with adjacent TCFs and or PTFs and users while activating or restoring circuits.

C5.5.4 After the tactical van equipment operators have aligned their systems, the control of system must be passed over to the TCF and or PTF, at which time the following are to be in effect:

C5.5.4.1 The TCF and PTF assumes full responsibility of the tactical circuits.

C5.5.4.2 The GIG CCSD trunk identifier must be used in both the GIG and tactical environment to identify each trunk and circuit.

C5.5.4.3 Tactical equipment operators must notify the TCF and or PTF of any known degradations or outages.

C5.5.4.4 The TCF and or PTF must report all GIG circuit and trunk outages, in accordance with DISAC 310-55-1 (reference 4.1).

C5.5.4.5 Any maintenance actions or removal of online equipment must be coordinated and approved by the TCF and or PTF.

Return to:

Chapter 5

Basic Circular

Top of Table of Contents

DISA Publication Listing

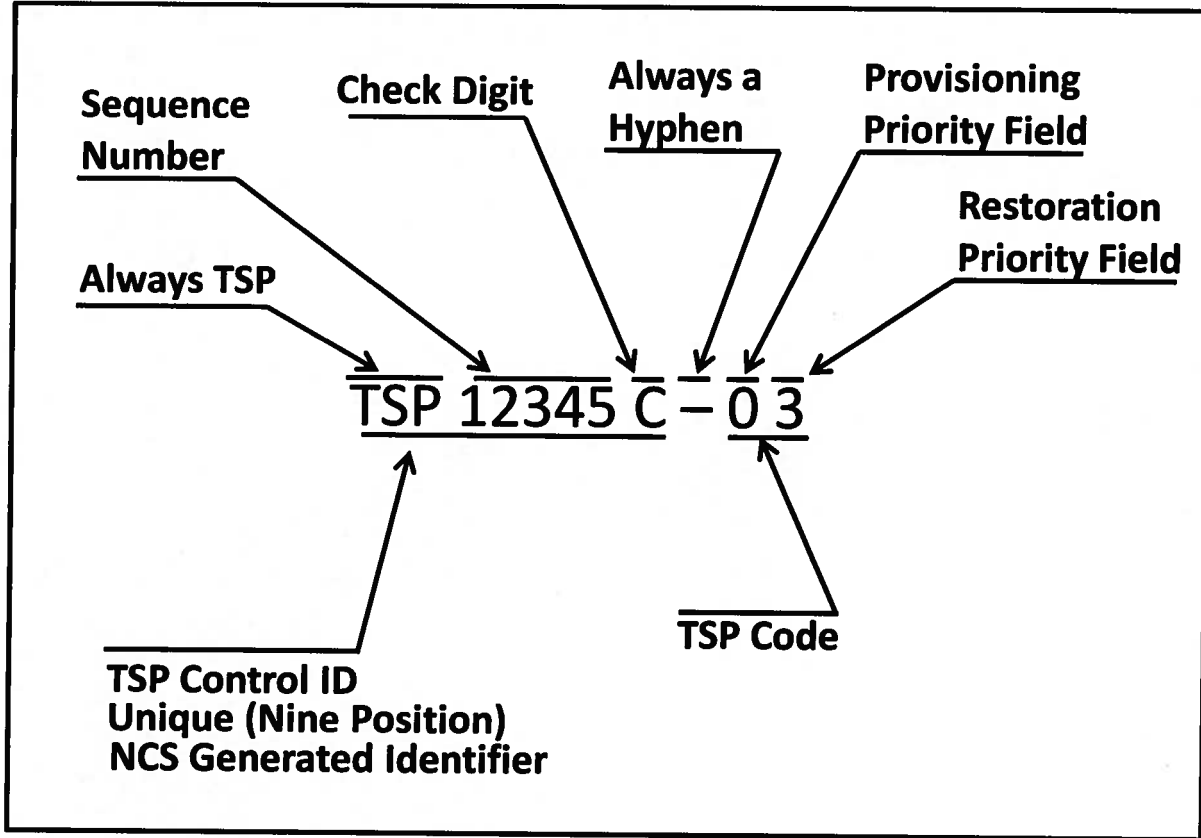
DISA Home Page

Continue to:

Chapter 6

DISA PUBLS@DISA.MIL - Last revision: 21 March 2012

FIGURE F5.1 TSP IDENTIFICATION CODE



Return to:
[Chapter 5](#)
[Basic Circular](#)
[Top of Table of Contents](#)
[DISA Publication Listing](#)
[DISA Home Page](#)

Continue to:
[Chapter 6](#)

DISA PUBS@DISA.MIL - Last revision: 21 March 2012

C6. CHAPTER 6. QUALITY CONTROL

C6.1 **General.** This chapter provides procedures for performing quality control (QC) on Global Information Grid (GIG) trunks and circuits and the application of established performance standards to those trunks and circuits. Performance of QC and applicability of performance standards encompasses three DISA numbered publications: this Circular (DISA Circular (DISAC) 310-70-1, which provides QC testing requirements; Supplement 1 to this Circular, Defense Information Infrastructure (DII) Technical Control Test Descriptions (reference 4.8), which provides detailed test descriptions for performing QC tests; and DISAC 300-175-9, Global Information Grid (GIG) Operating-Maintenance Electrical Performance Standards (reference 4.4), which provides test parameters and technical specifications for each type of trunk and circuit. Each GIG Technical Control Facility (TCF) and Patch and Test Facility (PTF) must maintain a copy of these Circulars for use by operation and maintenance (O&M) personnel responsible for supervising or performing test measurements of GIG trunks and circuits. GIG QC consists of in-service testing, out-of-service testing, and trend analysis. An efficient QC program may prevent interruption to user service by detecting and correcting adverse trends before user service is affected. Non-GIG facilities responsible for performing test measurements on GIG trunks and circuits that traverse their facility should also maintain a copy of the above numbered publications.

C6.1.1 To provide quality service to users of the GIG, each individual segment of the system must be operated and maintained at its optimum performance level. The method to achieve optimum performance is through effective QC.

C6.1.2 The two main types of QC testing prescribed in this chapter are in-service performance monitoring and out-of-service testing. Automated performance monitoring and or testing that satisfies requirements contained in this Circular and specifications contained in DISAC 300-175-9 (reference 4.4) is encouraged with a record copy of monitoring or testing results. Annual out-of-service QC tests are not required for digital circuits, as they are constantly monitored by network operations centers. However, initial test and acceptance (IT&A), as well as out-of-service testing for troubleshooting purposes, should be conducted in accordance with the circuit's parameter code standards, as identified in DISAC 300-175-9.

6.2 In-Service Performance Monitoring. The purpose of in-service performance monitoring is to provide performance information that indicates the quality of the operating signal traversing the network "without interruption" to the signal. In-service performance monitoring is mostly a manual function on analog systems whereas it is normally automated on digital systems. Automated in-service performance monitoring of digital systems may eventually negate the requirement to perform periodic out-of-service testing.

C6.2.1 In-service performance monitoring must be performed weekly on the send signal levels of all active analog circuits by each servicing TCF and PTF. Each servicing TCF and PTF must establish and maintain an in-service performance monitoring test schedule and work sheet for all analog circuits terminating at or traversing the GIG facility in a manner that provides trending information. Results will be recorded by exception. If a user's signal level is not within DISA specified standards or the circuit has an abnormal condition present, the tech controller should annotate the command communications circuit designator (CCSD), the signal level or abnormal condition, and the corrective actions taken. Significant problems should be documented in the Master Station Log (MSL). High impedance (e.g., 10K ohms) measurements are made at monitoring points to prevent interruption of user service. Normal user traffic signals, telephone supervisory signals, and composite transmission levels are some of the parameters which can be measured without interruption of service and compared to levels normally found at the transmission level point (TLP). Circuits must also be monitored for abnormal conditions (e.g., hybrid howl, cable hum) when user signals are not present. In-service performance monitoring must be performed as follows:

C6.2.1.1 On the transmit line monitor jack of the voice frequency (VF) patch bay, monitor the send signal level entering the transmission path. The transmit tolerance for signals originating from users at the local installation served by the TCF and PTF will be + .5 dB unless otherwise stated in DISAC 300-175-9 (reference 4.4). If an improper level is identified, the receive signal level at the cable patch bay (from the local user) should be checked. The faulty level must either be between the user and TCF and PTF or between the cable and VF patch bays within the TCF and PTF. Transmit tolerance for circuits originating at another facility that are routed through the TCF and PTF must be in accordance with link and multilink standards in DISAC 300-175-9 (+ 1 dB for single-link paths, + 2 dB for multi-link paths). If an improper level is

identified, the level of the receive signal from the cross-connect link should be checked to determine if the fault is in house or from another facility. Once the source of the faulty level is found, appropriate action must be taken to have it corrected. When troubleshooting problems that require signal adjustments, every facility along the entire transmission path must attempt to bring signals within + .5 dB.

C6.2.1.2 On the transmit line monitor jack of the cable (local user) patch bay, monitor the send signal level to the local user. Levels should be in accordance with link and multilink standards in DISAC 300-175-9 (+ 1 dB for single-link paths, + 2 dB for multilink paths). If an improper level is identified, the receive level from the transmission path should be checked to determine if the fault is in-house or from another facility. Once the source of the faulty level is found, appropriate action must be taken to have it corrected. When trouble-shooting problems that require signal adjustments, every facility must attempt to bring signals within + .5 dB along the entire transmission path.

C6.2.1.3 NE performance monitoring thresholds must be set in accordance with DISAC 300-175-9 (reference 4.4). If DISAC 300-175-9 does not contain appropriate thresholds, default values specified in equipment manuals must be used. If established thresholds cannot be met due to unique transmission equipment characteristics, then O&Ms may request site specific thresholds based on test and evaluation data. The request, as well as justification, must be submitted through the appropriate Facility Control Office (FCO) to the DISA Network Operations Center (DNC) transmission division for approval. If approved, the original data and justification must be maintained as long as nonstandard performance monitoring thresholds are being used.

C6.2.2 The concept within the digital environment is to utilize available in-service performance monitoring capabilities provided by network elements (NEs). The monitoring may be performed locally or at a centralized Network Management Center (NMC). Figure F6.1 shows typical GIG configurations using various NEs. As indicated, once a user signal traverses an NE, the signal is monitored by one or more higher level NEs. The performance information obtained from the NEs will indicate when degradation in performance occurs. Therefore, it is imperative that each GIG facility having NE equipment establish an effective in-service performance monitoring program.

C6.2.3 Each GIG facility with NE performance monitoring equipment must establish an in-service performance monitoring program using the following guidelines:

C6.2.3.1 Each GIG facility is to ensure NE alarm conditions are continually monitored. As a minimum, the alarm condition(s) of each NE should be verified every 2 hours. Although alarm conditions for each NE may be monitored by a centralized NMC, each GIG facility is still responsible for monitoring the NEs. NMCs do not necessarily receive all alarms generated from NEs. Completion of the alarm verifications must be documented. Any significant conditions, and corrective actions taken, should also be documented.

C6.2.3.2 Immediate action must be taken on service affecting alarm conditions (normally critical and major alarms). The appropriate FCO must be notified of any service affecting conditions. Normally, traffic will be rerouted and the degraded trunk or circuit taken out of service. Appropriate testing must be conducted to isolate and repair the fault.

C6.2.3.3 All other alarm conditions must be correlated with other data and corrected as soon as possible. Whenever in-service performance monitoring thresholds are exceeded, that particular trunk or circuit must be closely monitored and appropriate actions taken. If available, on-demand type monitoring should be implemented to provide additional data for fault isolation purposes.

C6.2.3.4 Historical alarm condition reports generated by each NE must be reviewed for each 24-hour period and maintained a minimum of 7 days. Corrective actions must be taken to correct abnormal trends.

C6.2.3.5 Performance reports generated by each NE must be reviewed for each 24-hour period and maintained a minimum of 7 days. These reports may be tailored by each facility to provide only that information necessary to perform an analysis of system performance. Corrective actions must be taken to correct abnormal trends.

C6.3 Out-of-Service Testing. Out-of-service testing bypasses the transmission media to allow complete access and end-to-end testing of the trunk or circuit. The purpose of out-of-service testing is to periodically verify the quality of prescribed specifications (in accordance with DISAC 300-175-9 (reference 4.4)) from terminal equipment to terminal equipment and to make

necessary end-to-end adjustments to interface and transmission equipment. Periodic end-to-end out-of-service testing must be performed in accordance with the following requirements on all GIG circuits and trunks assigned a parameter code unless a QC waiver conditions applies.

C6.3.1 GIG trunks or circuits that require special conditioning (e.g., C3, CT, and C5 parameter coded circuits), such as amplitude and delay equalizers to meet high speed transmission rates, require periodic out-of-service QC testing.

C6.3.2 Out-of-service testing is required for trunks and circuits when prudent (e.g., during degradations and customer complaints).

C6.3.3 Each servicing TCF and PTF should establish some form of periodic testing, or method to verify the signal quality, of those trunks and circuits that are extended from the TCF and PTF to remote user locations, traversing tail segments or that are extended off the installation.

C6.3.4 Segmented testing may be required when end-to-end performance of the trunk or circuit cannot be determined by normal end-to-end testing. An example is when a circuit traverses a mix (hybrid) of analog and digital transmission media where analog testing would be required on the analog segment(s) and digital testing would be required on the digital segment(s). Segmented testing may also be required when it is necessary to separate the circuit into identifiable segments, such as tail segments, transoceanic segments, U.S. Government-owned versus leased segments, etc., or for circuits assigned "Q" parameter codes as stated in C6.3.5.

C6.3.5 Hybrid circuits assigned a Q parameter code require segmented testing. Q parameter codes are normally assigned when the terminal device generates a digital signal that is converted through a modem, or other such device, to an analog signal for transmission. The Q parameter code should only be assigned when the modem is U.S. Government-furnished equipment (GFE), allowing government personnel test access to both the digital and analog side of the modem. An example of a typical Q parameter coded circuit is a Defense Message System (DMS) circuit. The DMS Switching Center generates a digital signal that normally traverses a DMS PTF. The digital signal is then converted at the DMS PTF to an analog signal, with a modem, for transmission to the primary TCF or to a commercial carrier. DISAC 300-175-9

prescribes specific analog and digital parameters applicable to each Q parameter code (e.g., a Q1 equates to a C1 and J1). (Refer to figure F6.2 for out-of-service testing diagram.)

C6.3.6 For T&A, Q parameter coded circuits must be tested for both parameter codes applicable to the circuit (e.g., Q1 circuits require testing for C1 and J1 parameters). The circuit must be tested for digital parameters end-to-end and then tested for analog parameters between the analog side of the modems. If the modem is located somewhere other than the TCF and PTF, and technical control personnel do not have access to the digital side of the modem, then a testing waiver should be granted for the digital test requirement. However, analog testing is still required. For Automatic Message Handling System (AMHS) circuits that have the modem installed at the AMHS PTF, the AMHS PTF is to perform end-to-end digital and analog testing. However, if the AMHS PTF is collocated with a primary TCF, the primary TCF should perform the analog testing if it is not economically feasible for the AMHS PTF to acquire a complete set of analog test equipment.

C6.3.7 Periodic out-of-service testing requires end-to-end digital tests. If the end-to-end digital tests fail specifications, then analog testing should be conducted to isolate any possible faults.

C6.3.8 The Communications Control Office (CCO) assigned to the trunk or circuit must schedule periodic out-of-service QC tests, as stated in subparagraph C6.3.3. The CCO schedules and maintains an out-of-service perpetual QC testing schedule for all trunks and circuits for which control responsibility is assigned. The CCO must ensure test schedules are fully coordinated with other required facilities and that a copy of the schedule is provided to those facilities.

C6.3.9 Periodic testing must be scheduled within the same month as when the circuit was activated. For example, if a circuit was activated in March 2012, then annual testing would be due anytime during March of successive years.

C6.3.10 Test schedules must be sufficiently flexible to allow for noncompletion due to reasons beyond the control of a facility. However, efforts must be made to ensure testing is completed within 30 days of the original activation date.

C6.3.11 QC testing performed in accordance with other DISA or O&M programs (e.g., DISA performance evaluations (PEs) and O&M inspections) or complete realignment of a trunk or circuit as the result of an outage will satisfy QC test requirements, if the testing is accomplished within 30 days of a scheduled QC.

C6.3.12 Out-of-service testing requires user release of the circuit if a reroute is not available. When testing multi-channel trunks (e.g., channel banks), the user release must be obtained from each user on the trunk.

C6.3.13 Circuits failing to meet parameter specifications during scheduled QC testing must be optimized and brought back within GIG parameter specifications. If the trunk or circuit cannot be brought back within specifications, the problem should be identified to the TSO issuing authority and the O&M for assistance.

C6.3.14 Those circuits not meeting GIG parameter specifications during the initial test and acceptance (T&A), but accepted for service, are only required to meet initial T&A test results. If T&A data is not available, the data from the first complete out-of-service QC test must be recorded and retained as T&A.

C6.3.15 Whenever T&A data is invalidated due to major realignment of equipment, change in transmission path, etc., the CCO must initiate end-to-end testing to establish new T&A baseline data.

C6.3.16 GIG facilities must develop QC procedures for testing local equipment if the procedures are not contained in another document. Training plans suffice if they contain procedures for testing local equipment.

C6.3.17 The sequence for digital parameters is not significant as most digital tests are performed simultaneously. The sequence of testing for analog parameters, however, must be performed in a logical sequence. Since most analog problems are level or noise sensitive, this is where testing should begin. Analog testing must be performed in the following sequence: net loss, idle channel noise, or C-notched noise; impulse noise (IPN) (with holding tone, if necessary); envelop delay, when applicable; frequency response; and all other required tests.

C6.3.18 A DD Form 1697: Circuit Parameter Test Data - Analog, or DD Form 1697-1: Circuit Parameter Test Data - Digital, will be used to record T&A and periodic QC data. TCFs and PTFs may use automated products in lieu of these forms if all the information required on the DD form(s) is contained in the substitute. The CCO and serving TCF and PTF must retain the DD Form 1697 or automated product on file in the circuit history folder. T&A data must be maintained for the life of the trunk or circuit. Periodic data must be maintained for all tests performed during the previous 12 months. Once the next annual QC test is performed, all previous periodic QC data may be discarded.

C6.3.19 All outages attributed to QC testing must be reported in accordance with DISAC 310-55-1, Status Reporting (reference 4.1), and Supplement 1 to 310-70-1, DII Technical Control Test Descriptions (reference 4.8).

C6.3.20 Out-of-service QC testing does not include time to troubleshoot and correct problems discovered during the QC test. When it is determined that a circuit does not meet the specified parameters and requires corrective action, the testing effort must be terminated. The circuit must be logged back "in" with the reason for outage (RFO) for authorized service interruption. A new "out" report must then be submitted with the actual reason for outage (e.g., defective equipment). The "out" time must be the same as the previous "in" time to reflect continuous outage.

C6.3.21 Scheduled QC testing is required for all communications equipment supporting GIG trunks and circuits, including spares. Communications equipment testing ensures the equipment meets the technical specifications contained in applicable technical manuals. All QC testing on communications equipment must be coordinated with the TCF and PTF supervisor on duty, whether the equipment is located in the TCF and PTF or another portion of the communications facility, in accordance with table 6.1 (analog) or table 6.2 (digital).

C6.3.22 Operational equipment is normally tested in accordance with O&M preventive maintenance procedures. Upon completion of any preventive maintenance, operational equipment must be tested in conjunction with TCF and PTF personnel before it is put back online.

C6.3.23 Spare communications equipment (e.g., conditioning equipment, multiplexers, and printers) with test access points appearing in the TCF and PTF must be scheduled for QC testing

by the TCF and PTF. Time interval used by O&M preventive maintenance procedures can be used as criteria for developing the schedule.

C6.4 Trend Analysis. Trend analysis must be performed at the lowest level possible where the customer interfaces with the GIG.

C6.4.1 All GIG TCF and PTFs must establish an aggressive trend analysis program on all circuits for which they are the Communications Control Office (CCO) or servicing TCF and PTF and on all trunks and links which terminate at their station. A Circuit Management Office (CMO) should also perform trend analysis for the circuits they are assigned responsibility. The program must trend number of outages, outage times, reason for outage, calculate availability and reliability, and determine if circuit reliability meets management thresholds (MT) on a monthly calendar basis. Availability and reliability includes all outages, including outages attributed to authorized service interruptions, switch outages, and preemptions (A, X or R in the first position of the DISAC 310-55-1 reason for outage [RFO] code). The formula to compute Availability as prescribed is $\% \text{ Availability} = 100 \times (\text{Total Time} - \text{Out Time}) / \text{Total Time}$. The formula to compute Reliability is $\% \text{ Reliability} = 100 \times (\text{Total Time} - (\text{Out Time} - \text{Excluded Time})) / \text{Total Time}$.

C6.4.1.1 MTs established in DISAC 310-130-2, Management Thresholds and Performance Objectives (reference 4.5) are categorized according to transmission media, network, or circuit restoration priority. These MTs must be used for trending GIG trunks and circuits. If a circuit is part of a specific GIG network that has MTs established for that network, then the MT for that network must be used for that circuit. All other circuits must use the MT established for circuit restoration priority.

C6.4.1.2 Anytime a link, trunk, or circuit fails monthly MT, the outages must be analyzed to determine if corrective actions are required. If a problem has been identified and additional action(s) cannot be taken (e.g., awaiting parts), then further actions are not necessary. Every effort must be made to ensure optimum reliability at all times.

C6.4.1.3 If a link, trunk, or circuit fails MT for two consecutive months and the problem has not been identified, the CCO and or servicing TCF and PTF must coordinate with the user and take appropriate actions to resolve the degradation. The CCO

and or serving TCF and PTF may have to perform QC tests on the user equipment, tail segment, and transmission system to isolate the fault. Once isolated, the problem must be turned over to the appropriate organization responsible for maintaining the specific equipment. If actions are not deemed necessary, the CCO and or serving TCF and PTF should document why further actions are not necessary (e.g., problem corrected). The CCO, or servicing TCF and PTF, must notify the appropriate FCO of all circuits, trunks, and links that fail MT for 2 consecutive months. Method of notification is at the discretion of the FCO. If the servicing TCF and PTF is not the CCO, the CCO must also be notified of each circuit on the list at which time the CCO should become involved with the problem.

C6.4.1.4 If the circuit fails MT for 3 or more consecutive months, the CCO, or servicing TCF and PTF, must take immediate action to improve circuit reliability, if action has not already been taken. Once the fault is isolated, or if the fault has already been isolated but not corrected, aggressive action must be taken to correct the situation. This may include involvement of the FCO, O&M command, or DISA. When assistance is required from DISA, the request should come from the FCO or O&M command. The CCO, or servicing TCF and PTF, must notify the appropriate FCO and O&M command of all links, trunks, and circuits that fail MT for 3 or more consecutive months. Method of notification is at the discretion of the FCO and O&M command.

C6.4.2 End-to-end testing, as used in this Circular, refers to the point nearest the user terminal equipment at each end of the trunk or circuit where a test point is accessible to perform required testing. The term "terminal equipment" refers to the physical location prescribed in the TSO where the terminal equipment is located. Ideally, the test access point should be at the user premises. The test access point may be physically accessed (e.g., patch panel and main frame) or electronically accessed (e.g., Promina, DISN Asynchronous Transfer Mode Services (DATMS), and internet protocol (IP) routers, matrix switches, and Defense Switched Network (DSN) Multiprotocol Label Terminal (MAP) terminal). When testing at a location other than a TCF and PTF where normal patching facilities are not available, modified test procedures may be required (e.g., test equipment may have to be connected to the terminal equipment or a main frame using clips or test probes). Removal of wires from user terminal equipment or the user main frame should not be accomplished without permission of the user and any contractor

responsible for maintenance of the equipment. If in doubt, do not modify equipment installation for testing; conduct the testing at the nearest test access point.

C6.4.3 Performance of QC testing is an inherent function of every GIG facility (e.g., TCF and PTF, microwave, switching facility, and satellite terminal) that has GIG circuits routed through the facility. Individuals in charge of GIG facilities must ensure trained personnel are available during every shift to perform scheduled and unscheduled QC testing. Although some facilities have a "quality control section" established as part of their staff, shift personnel must still be capable of performing QC tests. The TCF and PTF shift supervisor is responsible for ensuring scheduled testing is completed and every effort is made to conduct unscheduled testing, as necessary. When testing is required at an unmanned facility, the Communications Control Office (CCO) must coordinate with the TCF and PTF responsible for the unmanned facility to ensure personnel are available at the unmanned facility for testing.

C6.4.4 Every effort must be made to ensure all required test equipment is available and is calibrated for conducting QC testing. If required test equipment is not available, appropriate actions must be taken to postpone or reschedule to a time when all test equipment is available. Each TCF and PTF must maintain an up-to-date status of available test equipment with calibration status and actively pursue replacement of nonavailable test equipment. Each O&M is to ensure their facilities have the necessary test equipment to perform in-service and out-service required tests detailed in this chapter and that the test equipment is compatible with other GIG facilities. When an item of test equipment is inoperative or turned in for recalibration and a compatible substitute is not available, the test equipment should be declared "mission essential" and an attempt made to obtain a replacement so that fault isolation, QC, and performance monitoring functions are not impaired.

C6.5 **Test Tone Power Levels.** The standard test tone power level for testing voice frequency GIG circuits is -10 dBm0 at 1004 Hz. Tests at this power level should be limited to 30 minutes or less. If a standard test tone is required for longer than 30 minutes, the level should be reduced to a -15 dBm0.

C6.5.1 Certain test equipment (e.g., portable test sets) may not have the capability to provide a standard test tone frequency of 1004 Hz. When the standard test tone frequency is not available, an alternate test tone frequency of 1010 Hz may be used. Use of test tone power levels higher than the standard level is permissible whenever such tests are required to measure parameters that are level sensitive. Such tests are permitted only on systems which are out of service or during nonbusy hours to minimize degradation to other users of the system. The use of nonstandard test tone levels is also permissible whenever testing leased commercial facilities and the carrier representative requests a specified level.

C6.5.2 When testing leased circuits with commercial carriers, the TCF and PTF may utilize a test tone at data level (e.g., -13 dBm0) if the commercial carrier requests that this be done. The TCF and PTF must be aware that the commercial carrier transmission level point (TLP) may be different than the GIG TLP. It is advisable to check with the local commercial carrier to determine the proper test tone level and frequency.

C6.6 Excessive Signal Levels. Excessive signal levels are frequently introduced into the GIG from user equipment, misaligned conditioning equipment, and transmission equipment, etc. Excessive signal levels are normally detected during in-service monitoring. Detection and correction of excessive signal levels interfacing with time division multiplexing (TDM) systems is equally important to prevent signal clipping and degradation. Whenever any excessive signal level(s) are detected, immediate action must be initiated to locate the source and correct the level. The serving TCF and PTF must immediately notify the user or other TCF and PTF that is originating the excessive signal level and request immediate action be taken to correct the level. The TCF and PTF must take appropriate actions to include denial of service, if necessary. Action of this nature must be properly documented and immediately reported to the appropriate Facility Control Office (FCO). Denial of service for the above reason will be exercised judiciously according to the following guidelines:

C6.6.1 In all situations, the TCF and PTF should attempt to reduce excessive signal levels by use of pads, attenuators, or other devices until permanent corrective action can be taken.

C6.6.2 The normal speech level for voice is -10 dBm0 with peaks to 0 dBm0. Maximum voice peaks should not exceed +5 dBm0 more than 15 times per 15 minute period. If a voice circuit

is peaking above 0 dBm0, refer to the maximum operating signal level test, contained in Supplement 1 to this Circular (reference 4.8), for procedures. If the circuit fails the maximum operating signal test, immediate action must be taken to correct the level or remove the circuit from the transmission path.

C6.6.3 For circuits with constant levels, the standard signal level should be -10 dbm0, in accordance with DISAC 300-175-9 (reference 4.4) (e.g., Dual Frequency Idle Tone, 2800/2600 Hz, should be -20 dBm0; data levels should be -13 dBm0). Anytime the signal level exceeds the standard by 3 dB or more, the level must be corrected as soon as possible. Anytime the signal level exceeds the standard by 6 dB or more, the level should be corrected immediately or taken out of service.

C6.7 Test and Acceptance (T&A) Testing. T&A testing is also an important part of testing under CQ management. All GIG circuits and trunks assigned parameter codes must be tested prior to acceptance for service by the U.S. Government, unless a waiver condition applies. The CCO and CMO assigned in the TSO is to ensure T&A testing is completed. (Refer to paragraph C6.9 for waiver conditions.)

C6.7.1 The CCO and CMO must ensure the required in-effect, delayed service, or exception reports are submitted upon completion of the T&A test, in accordance with DISAC 310-130-1, Submission of Telecommunications Service Requests (reference 4.6).

C6.7.2 The TSO issuing authority may grant a temporary T&A waiver when cutting over existing circuits in support of a major project. When a temporary T&A waiver is issued, T&A testing must be performed during the next scheduled periodic out-of-service QC, or within 180 days, whichever is sooner.

C6.7.3 Trunks or circuits that do not have government test access points (e.g., commercially provided end-to-end) are waived for T&A testing. The CCO and CMO are to verify U.S. Government test access points do not exist. The trunk or circuit should be in-effect once the user advises that the requested service has been provided and that service is satisfactory, in accordance with the TSO and any contractual documents.

C6.7.4 Trunks or circuits failing to meet any test parameter specification during T&A testing will not be accepted for service by the U.S. Government. When a trunk or circuit fails to meet specifications, an exception report must be submitted. The CCO and CMO will include extracts from the appropriate portions of a DD Form 1697: Circuit Parameter Test Data, in the exception that extracts will include identification of any tests where a parameter failed to meet specifications, specific measurements obtained, and other appropriate comments.

C6.7.5 Once notified that a trunk or circuit does not meet T&A test parameter specifications, the TSO issuing authority must determine, or will require the requestor to determine, if the measured parameter specifications are adequate to meet user requirements. If the parameter specifications are determined to be adequate, the CCO and CMO may be directed to accept service on behalf of the U.S. Government. The TSO issuing authority or requestor must advise whether service will be temporarily accepted until the parameter(s) are corrected, in which case an exception report must be submitted, or whether service is to be permanently accepted with the degraded parameter(s), in which case an in-effect report must be submitted. If the parameter specifications are not adequate, the circuit will not be accepted for service until satisfactory service can be provided. Any necessary technical or equipment procurement assistance to correct local problems is to be provided by the O&M. If the problem is determined to be with the circuit design, engineering assistance is to be provided by DISA.

C6.7.6 If the TSO issuing authority or the requestor determines the service is satisfactory and service is to be accepted, the initial T&A data will be used as the baseline for future testing.

C6.7.7 The CCO and CMO must maintain current listings of circuits that were accepted for service but not meeting required parameters and must ensure outstanding exception(s) are cleared by an in-effect report at the earliest possible date. The CCO and CMO must submit followup reports every 30 days until the exception(s) are cleared. (Refer to chapter 8 for specifics.)

C6.8 Equipment Test and Acceptance Test. Technical and operational compatibility of all equipment interfacing with the GIG is imperative to providing reliable and quality service. Therefore, technical control personnel must be involved with

installation and T&A teams responsible for accepting GIG communications systems and subsystems. TCFs and PTFs are to coordinate with other GIG facilities concerning the addition of new equipment into the system and to perform appropriate QC tests on the new equipment to ensure it is capable of supporting user service. If the design capability of the equipment permits satisfactory operation at lower specifications than those specified in DISAC 300-175-9 (reference 4.4), then the specifications contained in the equipment technical manual may be used. Test results must be maintained until such equipment is removed.

C6.9 Waivers. Waivers may be granted for T&A, and for periodic out-of-service testing, if the capability for testing does not exist. QC waivers can be obtained from DISA in the original Telecommunications Service Order (TSO), after the TSO has been issued or for any of the conditions listed that the CCO and CMO determines justifiable. The CCO and CMO is responsible for maintaining a complete list of all circuits that are waived from testing (T&A and or periodic). The waiver list must be available to personnel responsible for performing QC tests and must include the reason for the waiver and the effective date. Each circuit added to the waiver list must be validated by the facility chief. Circuits must be deleted from the list anytime the condition that caused the waiver changes. The entire waiver list must be revalidated annually by the facility chief and be submitted to the highest level O&M command within their area, and to the appropriate FCO, for review during the first quarter of each calendar year. Waiver lists must be provided to DISA upon request. The list and waiver conditions are subject to review during DISA or O&M evaluations.

C6.9.1 If it is known at any organizational level within the Telecommunications Request (TR) and TSO process that the capability to test the circuit will not exist, a QC waiver may be included as part of the TR and TSO. Although testing capabilities may not be known at the TR level, there are cases involving specialized circuits where it is known that testing will not be performed. In these cases, the requesting organization may include the waiver request in the TR. If a waiver is not requested in the TR, the DISA allocation and engineering (A&E) activity is authorized to provide a test waiver in the TSO, if the DISA A&E activity is aware or can verify with the O&M organization responsible for testing that testing capability will not exist. The waiver should be

included in paragraph 5 of the TSO. Inclusion of a waiver in the TSO precludes the necessity of issuing an administrative waiver once the circuit is activated.

C6.9.2 Once a TSO is issued without a waiver, it becomes the accountability the CCO and CMO to justify a waiver or to obtain a waiver from DISA when conditions warrant. Chapter 77 of DISAC 310-65-1, Circuit and Trunk File Data Elements and Codes Manual of the Global Information Grid (GIG) (reference 4.9), contains a listing of available waiver codes. Detailed justification must be provided when requesting a waiver from DISA. The CCO and CMO designated in the TSO must identify the specific circumstances pertaining to each waiver request to their O&M command for concurrence or nonoccurrence. If the O&M concurs, the O&M must forward the request to the appropriate DNC approval authority (DISA Europe [DISA-EUR], DISA Pacific [DISA-PAC], and DNC) with an information copy to the appropriate requestor. Waiver requests on circuits traversing more than one DNC will be granted by the DNC approval authority that has jurisdiction over the CCO and CMO, after coordination with the other DNCs. Copies of waiver-related correspondence must be retained in the circuit history folder.

C6.9.3 The CCO and CMO may apply any of the following conditions once the CCO and CMO has verified that the condition exists and once the facility chief validates the waiver. Any condition other than the following requires approval from DISA and a waiver must be requested through the DISA allocation and engineering activity outlined in the TR or TSO.

C6.9.3.1 Circuits that cannot be tested due to lack of test point(s) accessible by government personnel are waived for T&A and periodic testing. This includes end-to-end commercially leased circuits that do not traverse government facilities. If the waiver is not included in the TSO, the CCO and CMO must verify that test access points are not available or that the circuit does not traverse any government facility before waiving test requirements.

C6.9.3.2 IP router networks circuits are waived from periodic testing. T&A testing must be performed before accepting service. Once the circuit is accepted for service, internet protocol (IP) router network circuits will only be quality controlled when directed by the appropriate IP router networks monitoring center. Routine QC is the responsibility of the appropriate IP router network monitoring center utilizing installed software.

C6.9.3.3 Any circuit assigned a service availability code where an electrical path is not available until the circuit is activated is waived for periodic testing. T&A testing must be accomplished.

Return to:

Chapter 5

Basic Circular

Top of Table of Contents

DISA Publication Listing

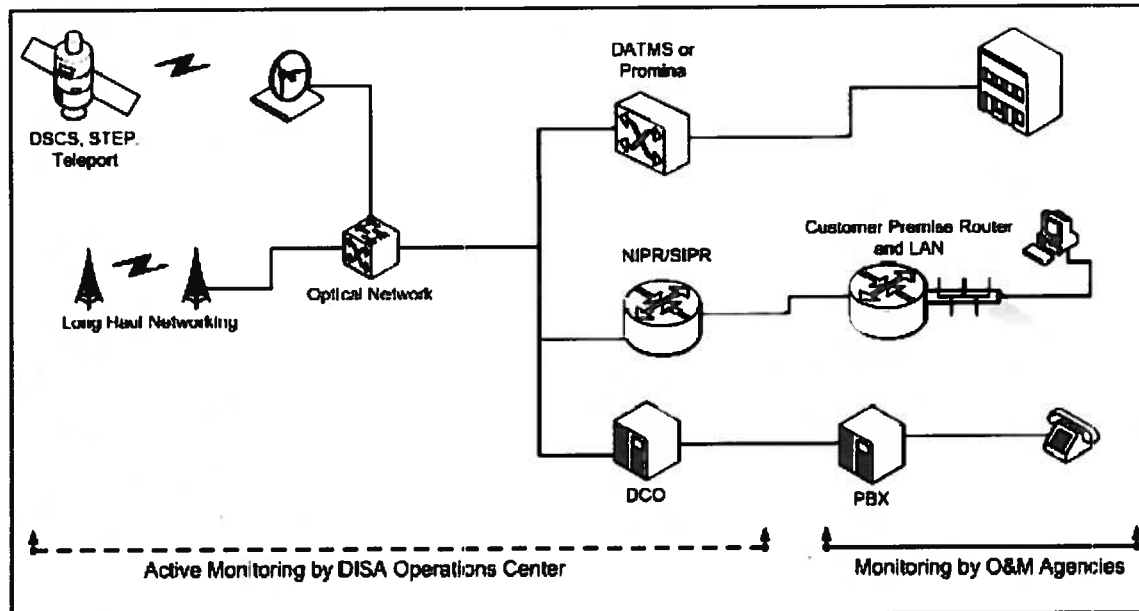
DISA Home Page

Continue to:

Chapter 8

DISA PUBS@DISA.MIL - Last change: 21 March 2012

Figure F6.1 Network Element Performance Monitoring



Return to:

[Chapter 5](#)

[Basic Circular](#)

[Top of Table of Contents](#)

[DISA Publication Listing](#)

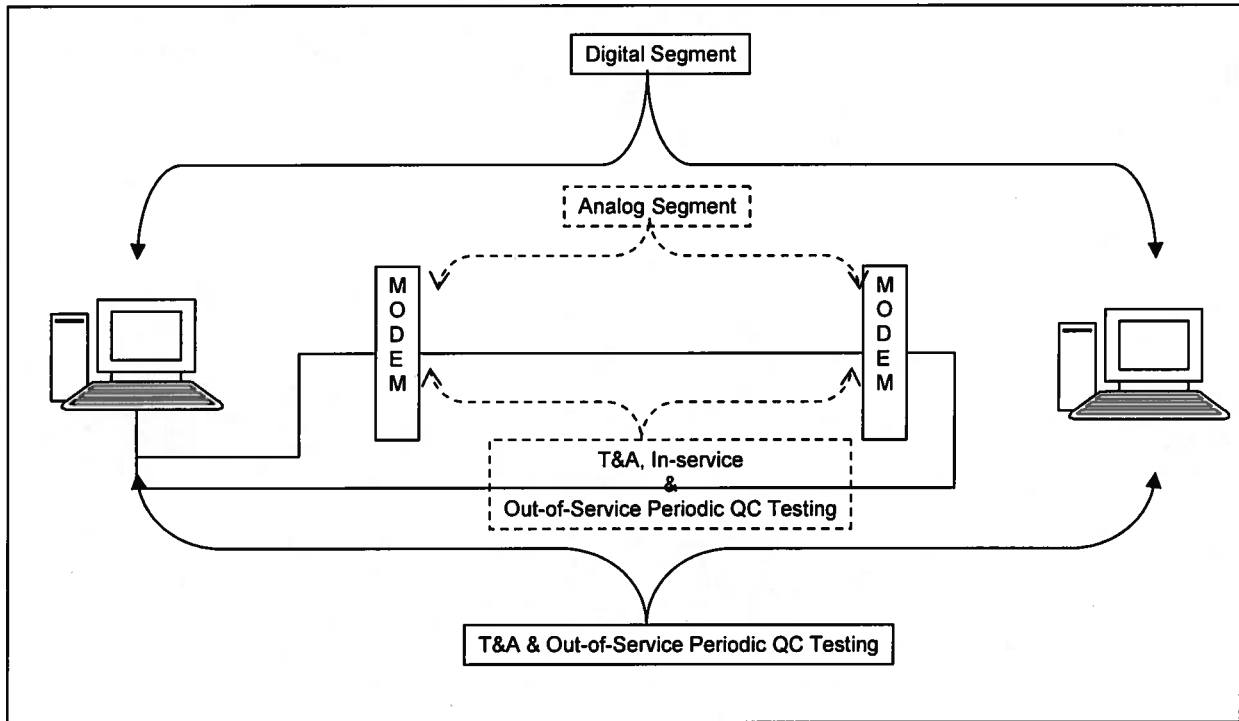
[DISA Home Page](#)

Continue to:

[Chapter 8](#)

DISA PUBS@DISA.MIL - Last change: 21 March 2012

Figure F6.2 Q Parameter Segmented Testing



Return to:

[Chapter 5](#)

[Basic Circular](#)

[Top of Table of Contents](#)

[DISA Publication Listing](#)

[DISA Home Page](#)

Continue to:

[Chapter 8](#)

DISA PUBLS@DISA.MIL - Last change: 21 March 2012

TABLE T6.1 Analog Circuit Quality Control Test Schedule

| Parameter Codes | C0*2 C4 | C1 M1 | C2 M2 | C3 D1 | C5 D6 | CT M3 |
|------------------------------------|------------|----------|----------|----------|----------|----------|
| Frequency | T&A | IN | OUT | T&A | IN | OUT |
| Test Parameter | | | | | | |
| Transmission Level*3 | | W | | | W | |
| Net Loss | | | A | | | SA |
| C-Message Noise or C-notched noise | | | A | | | SA |
| Signal to C-Notched Noise Ratio | | | A | | | SA |
| Impulse Noise | | | A | | | SA |
| Envelope Delay | | | A | | | SA |
| Frequency Response | | | A | | | SA |
| Max Change in Audio Frequency | | | A | | | SA |
| Maxtime Net Loss Variation | | | AR | | | AR |
| Terminal Impedance | | | AR | | | AR |
| Nonlinear Distortion*4 | | | AR | | | AR |
| Phase Jitter*4 | | | AR | | | AR |
| Gain Hits*4 | | | AR | | | AR |
| Phase Hits*4 | | | AR | | | AR |
| Drop Outs*4 | | | AR | | | AR |
| Gain Linearity at Input*4 | | | AR | | | AR |
| Signal to Quantizing Distortion*4 | | | AR | | | AR |
| Circuit Continuity*4 | | | AR | | | AR |
| Cross Modulation*4 | | | AR | | | AR |
| Maxium Operating Signal Level*4 | | | AR | | | AR |

***Note: * represents scientific notation for following number ***

Return to:

- [Chapter 5](#)
- [Basic Circular](#)
- [Top of Table of Contents](#)
- [DISA Publication Listing](#)
- [DISA Home Page](#)

Continue to:

- [Chapter 8](#)

DISA PUBS@DISA.MIL - Last change: 21 March 2012

Table T6.2 Digital Circuit Quality Control Test Schedule

| Parameter Codes | Y1 | Y2 | Y3 | Y4 | J2 | J5 | J1 | J3 | N1 | | |
|---------------------------------|-----|----|-----|-----|----|-----|-----|-----|-----|----|-----|
| | S1 | S2 | S3 | S4 | | J4 | W1 | | | | |
| Frequency | T&A | | OUT | T&A | | OUT | T&A | OUT | T&A | IN | OUT |
| Test Parameter | | | | | | | | | | | |
| Bit Error Rate | | | AR | | | SA | | A | | | |
| % Error Free Sec | | | AR | | | SA | | A | | | |
| Availability | | | AR | | | AR | | AR | | | |
| % Block Error | | | AR | | | AR | | AR | | | |
| Jitter | | | AR | | | AR | | AR | | | |
| Loss of Bit Count | | | AR | | | AR | | AR | | | |
| Integrity (LBC) | | | | | | | | | | | |
| Sync Time | | | | | | AR | | | | | |
| Interchannel | | | | | | AR | | | | | |
| Differential | | | | | | | | | | | |
| Delay | | | | | | | | | | | |
| Loop Transport | | | | | | AR | | | | | |
| Delay | | | | | | | | | | | |
| Total Peak | | | | | | | | | | W | AR |
| Telegraph Dist | | | | | | | | | | | |
| Bias Distortion (Mark/Space) | | | | | | | | | | | AR |

Return to:

Chapter 5

Basic Circular

Top of Table of Contents

DISA Publication Listing

DISA Home Page

Continue to:

Chapter 8

DISA PUBL@DISA.MIL - Last change: 21 March 2012

C8. CHAPTER 8. SERVICE PROVISIONING

C8.1 **General.** This chapter describes the procedures necessary to start, change, amend, or discontinue the various basic types of services and circuits in the Global Information Grid (GIG), as prescribed by DISAC 310-130-1, Submission of Telecommunications Service Requests (reference 4.6). Refer to DISAC 310-130-1 for detailed information on other types of services. The basic circuit design information for all new or changed circuits will be provided in Telecommunications Service Orders (TSOs). The TSO may also be used as the authority for the operation and maintenance (O&M) agency to procure specific devices and ancillary equipment necessary to install the circuit or service at a GIG facility. To accomplish the very close coordination required to activate circuits in the GIG, a Communications Control Office (CCO) or Circuit Management Office (CMO) is normally assigned responsibility for activating the circuit from end-to-end. Intermediate facilities are assigned the responsibility for coordinating all actions necessary to activate the circuit within their facility, keeping the CCO and CMO advised of all actions taken. All GIG facilities have the continuing responsibility for maintaining the circuits terminating at or traversing their facility at the highest possible level of performance. Although procedures in this chapter describe circuit activation, these same procedures apply to activation of all GIG services.

C8.2 **Telecommunications Service Order (TSO).** The TSO is the official document issued by a DISA Provisioning Center to start, change, amend, or discontinue circuits, trunks, links, or systems; to amend previously issued TSOs; and to affect administrative changes. Changes to circuit configurations are normally not authorized without an approved TSO from a DISA Provisioning Center. Verbal TSOs or Operational Directive Messages (ODMs) are issued when there is insufficient time to prepare and distribute a record TSO. A record TSO will be issued within 5 working days of the ODM issuance. The following explanations are provided for a TSO. (Refer to figure F8.1 for a sample TSO.)

C8.2.1 **Numbering.** Each TSO is assigned an alpha/numeric TSO number (e.g., D2474/26WU-01) derived as follows:

C8.2.1.1 The beginning letter designates the issuing Provisioning Center: DISA Headquarters - C, D; DISA-Europe - E, F, G, H, Y; DISA Pacific P, Q; and DISA CONUS - A, B, T, X, or W.

C8.2.1.2 The first digit designates the year in which the TSO is issued; such as, 2 for 2012.

C8.2.1.3 The next four digits represent sequential TSO serial numbering within the calendar year beginning 1 January.

C8.2.1.4 Following the back slash are the last four characters (circuit number) for the command communications service designation (CCSD) of the circuit or the entire six-character designator of the trunk being acted upon.

C8.2.1.5 Following the dash is a two-digit number to identify the sequential action being taken on the circuit or trunk since its inception. The number 01 is used as the first action or start; numbers 02 through 98 are used in sequential order to indicate changes with discontinuance of the service as a last action identified with 99.

C8.2.2 **Format.** The TSO is prepared for electrical transmission in message format. Subparagraphs C8.2.2.1 through C8.2.2.4 describe the entries for each paragraph of the TSO and are keyed to like-numbered paragraphs and subparagraphs of the TSO.

C8.2.2.1 **Subject.** TSO number (TSO D2474/26WU-01).

C8.2.2.2 **References.** Message or letter identification of those items directly related to the TSO(s).

C8.2.2.3 **Paragraph 1.**

C8.2.2.3.1 [1A] States the purpose of the TSO in short concise terms (e.g., "This TSO is issued to establish Predator Service" or "This TSO is issued to amend TSO D60019/A350-01").

C8.2.2.3.2 [1B] Used for TSO coordination.

C8.2.2.3.3 [1C] Used for DISA control number.

C8.2.2.4 **Paragraph 2.** General circuit or trunk information used by the Technical Control Facility (TCF) and Patch and Test Facility (PTF) for preparing circuit records and by DISA for updating the circuit and trunk files in the GIG data base. Subparagraphs C8.2.2.4.1 through C8.2.2.4.28 are keyed to like-numbered paragraphs and subparagraphs of the TSO. Descriptions of coded entries are contained in DISAC 310-65-1, Circuit and Trunk File Data Elements and Codes Manual of the Global Information Grid (GIG) (reference 4.9).

C8.2.2.4.1 [2A] CCSD or trunk identification (ID).
If changing from one CCSD to another or from one trunk ID to another, the old CCSD is listed first and the new CCSD is identified after the diagonal slash (/).

C8.2.2.4.2 [2B] National Communications System (NCS) Telecommunications Service Priority (TSP) authorization code. The TSP authorization code has 12 positions. Positions 1 through 9 is a TSP control ID used by the NCS. Positions 11 and 12 are the TSP provisioning and restoration priority codes. An example of a TSP authorization code would be "TSP12345C-03." Refer to Figure F5.1 and DISAC 310-130-4, Defense User's Guide to the Telecommunications Service Priority (TSP) System (reference 4.7), for detailed information.

C8.2.2.4.3 [2C] Type of action; e.g., start, change, amend, or discontinue.

C8.2.2.4.4 [2D] Service date by day, time (ZULU), month, year (e.g., 010001Z JAN 12. For temporary service (30 days or less) or for exercise circuits, the discontinue date and time (optional) will be entered in the second set of blocks. (The service date and discontinue date must be separated by the word "THRU.")

C8.2.2.4.5 [2E] User terminal locations by contracted geographical location (GEOLOC), user terminal code, facility code (FAC), state and country code, and GIG area code. Included are user contacts at each terminal by name or title, telephone number, and e-mail address. Commercial and Defense Switched Network (DSN) telephone numbers for commercial carriers are provided, if possible.

C8.2.2.4.6 [2F] Circuit parameter code (in accordance with technical schedules in DISAC 300-175-9, Global Information Grid (GIG) Operating-Maintenance Electrical Performance Standards (reference 4.4)).

C8.2.2.4.7 [2G] Type operation (e.g., full duplex, half duplex).

C8.2.2.4.8 [2H] Control office by type, GEOLOC, and en route facility code (e.g., CCO, CMO, Intermediate Control Office [ICO]).

C8.2.2.4.9 [2I] Circuit modulation rate (e.g., 60 Mbps) or trunk channel capacity (e.g., 12 channels).

- C8.2.2.4.10 [2J] Security equipment nomenclature short title (e.g., KG-194, , KG-175E, Thales, SAFENET, TACLANE, etc.).
- C8.2.2.4.11 [2K] Service availability (e.g., full period, on-call).
- C8.2.2.4.12 [2L] Signaling mode (e.g., 2-way dial, 2-way ring-down) or trunk channel capacity (e.g., 12 channels) or trunk bandwidth or bit rate in trunk TSOs.
- C8.2.2.4.13 [2M] Trunk mileage for trunk TSOs.
- C8.2.2.4.14 [2N] TSR number assigned by the requestor via DISA Direct Order Entry (DDOE) whose mission the circuit supports (e.g., DU24APR910772).
- C8.2.2.4.15 [2O] Trunk or circuit cross-reference (e.g., CCSD and trunk number assigned to package system trunk).
- C8.2.2.4.16 [2P] Circuit or trunk set identification code. This is a Worldwide On-Line System (WWOLS) computer generated field. Used to identify the database set in the circuit or trunk files. For starts, "A" is used; for changes, the next alpha character following the one in the current file is used.
- C8.2.2.4.17 {2Q} Circuit Routing Code. Used by DISA circuit allocators and engineers to identify whether or not the circuit is routed in an optimum manner.
- C8.2.2.4.18 [2R] Program Designator Code (PDC). Funding code provided by the requestor for billing purposes on leased circuits or circuits under industrial funding.
- C8.2.2.4.19 [2S] DoD code for agency requiring service.
- C8.2.2.4.20 [2T] Diverse routing. The circuit number (last four characters of CCSD) of up to three circuits from which the requested service described in the TSO must be diversely routed.
- C8.2.2.4.21 [2U] Avoidance routing and transmission media avoidance.
- C8.2.2.4.21.1 Avoidance routing. Contracted GEOLoc and associated state and country codes of locations which must be avoided by this circuit.

C8.2.2.4.21.2 Transmission media avoidance. Specific types of transmission media which must be avoided by this circuit.

C8.2.2.4.22 [2V] Not Used

C8.2.2.4.23 [2W] Not used

C8.2.2.4.24 [2X] Type trunk modulation. The type of modulation used on the transmission pathway between the two terminals of a trunk (e.g., dense wavelength division multiplexing (DWDM), time division multiplexing (TDM). This paragraph is "NA" for circuit TSOs.

C8.2.2.4.25 [2Y] Not Used

C8.2.2.4.26 [2Z] Not Used

C8.2.2.4.27 [2AA] Sequence data base (SDB) Number. Wideband Satellite Communications (SATCOM) Operations Center (WSOC) service.

C8.2.2.4.28 [2AB] Not Used

C8.2.2.5 Paragraph 3. Facility and circuit equipment information or facility and trunk equipment information. This paragraph contains information on each facility through which the circuit or trunk is routed. Trunk routing information includes the link over which the trunk is routed, where applicable. The paragraph includes the equipment, to include encryption to be used at each facility, the interface specification, signaling details, and logical signal flow of the circuit.

C8.2.2.5.1 Facility by contracted GEOLoc, state and country code, terminal or en route facility (FAC) code, multipoint code, and Intermediate Control Office (ICO) or no data base entry (NDB), as appropriate, followed by building and room number, and the typical configuration code. A to Z direction would be from the first facility listed under paragraph 3 to the last facility listed under paragraph 3 (e.g., paragraph 3a to paragraph 3z). Z to A would be in the opposite direction. A to Z equates to direction one in the DISA data base circuit file; Z to A equates to direction two.

C8.2.2.5.1.2 Trunk or Link Information, paragraph 3X2A. For circuit TSOs, the trunk designator and the channel to which the circuit is allocated are shown. Also, the type signaling,

(supervisory, on-hook, off-hook) commercial circuit number, type segment, alternate PDC, and type operation, as appropriate. For trunk TSOs, the link designator for the trunk is shown.

C8.2.2.5.1.3 Trunk or Link Information 3X2B. Explanatory remarks are provided, as required for circuit orders. Trunk TSOs will use this paragraph to identify the type media, trunk cross-reference, and link mileage between terminals.

C8.2.2.5.1.4 Trunk or link information paragraph 3X2C. Contains cross reference to another nation's circuit identifier when a particular portion of a circuit is routed over another nation's system.

C8.2.2.5.1.5 Paragraph 3X2F (PROMINA): Domain and or Node assignment, if applicable.

C8.2.2.5.1.6 Paragraph 3X2G (Router): Node ID assignment for DISN internet protocol (IP) services requirements, if applicable.

C8.2.2.5.1.7 Paragraph 3X2I (System Trace) (STM): Node ID assignment for Fort Buckner circuit actions, if applicable.

C8.2.2.5.1.8 Paragraph 3X2J. (Asynchronous Transfer Mode) (ATM): Annotate the Node Identification (ID), if applicable.

C8.2.2.5.1.9 Paragraph 3X2K. (SR): Service request (SR) and service order (SO) numbers of the Joint Hawaii Information Transfer System (JHITS) request order.

C8.2.2.5.2 For multipoint circuits, TSOs are written from one user terminal to a bridge point and then to a distant user. The bridge point is repeated and another subscriber added, either directly or through another bridge point and so on, until all users are described. The multipoint code behind a specific GEOLOC, state and country code, and en route and facility code indicates whether a terminal or hubbing point is at that location.

C8.2.2.6 Paragraph 4. Other specified data.

C8.2.2.6.1 [4A] Channel Designations. This paragraph is used to tell computer software to build trunk channel records.

C8.2.2.6.2 [4B] Not used

C8.2.2.6.3 [4C] Trunk and channel numbers released.

C8.2.2.6.4 [4D] Central Conference Communication Initiative (CCCI) and Allied Long Lines Agency (ALLA) numbers discontinued. (Note: TSO paragraphs 4E-4J are used in trunk TSOs for entry of trunk Port Channel Engineering (PCE) information.)

C8.2.2.7 **Paragraph 5.** Other specific directions to include are as follows:

C8.2.2.7.1 Statement(s) to direct testing, direct submission of completion reports, establish proper levels, or cover interface requirements.

C8.2.2.7.2 Directions to the leasing agency.

C8.2.2.7.3 Data base responsibility.

C8.2.2.7.5 Any other narrative data that will help ensure understanding of the circuit or trunk to which the TSO pertains.

C8.2.2.7.6 Statement(s) used by the DISA computer program to set the type of data field for either automatic or contingency execution on the date specified in the TSO.

C8.2.2.7.7 Statement(s) used to assist Defense information Technology Contracting Organization (DITCO) in automatically processing TSOs.

C8.2.2.7.8 Statement(s) pertaining to test and acceptance and quality control.

C8.2.2.10 **Paragraph 8.** GIG Switched Record Network (IP Router Networks). Paragraph 8 is used by DISA advance encryption (AE) standard during development of the TSO. The information contained in paragraph 8 is converted and appears as paragraph 6 in the TSO. Information will include [8L] Crypto Account Number, [8M] Crypto account Custodian, [8N] Crypto Account Custodian Mailing Address, and [8O] Crypto Account Custodian Defense Message System (DMS) address.

C8.2.3 **Distribution.** The TSO is normally sent for action to each user, GIG facility on the trunk or circuit; the designated GIG control office; the leasing agency, if applicable; and the other DISA circuit allocation and engineering (A&E) offices if the trunk or circuit enters their area of responsibility (AOR). An information copy of the TSO is also sent to the operation

and maintenance (O&M) agency headquarters of the GIG facilities, the requestor, and the using agency of the circuit. Additional distribution will be made only as necessary to meet specific requirements that may arise within a DISA Network Operations Center (DNC) or to support a major project wherein engineering or logistic considerations are involved.

C8.3 Circuit Installation, Alignment, Testing, Certification, and Deactivation. The many variations found in the configurations of GIG facilities prevent the development of standard procedures which could apply to all types of circuits and to every GIG facility. However, there are certain functional steps in activating circuits which are common to all facilities. Upon receipt of a TSO, the following should be accomplished: the TSO should be administratively processed and receipt logged; determination should be made from all concerned, including users, of the capability to provide service as specified in the TSO; the detailed in-facility layout designating specific cross-connects and specific equipment to be used as required by the TSO should be prepared; and work orders, or instructions, to personnel or work centers responsible for performing in-facility configuration should be prepared.

C8.3.1 Installation. Performance of in-facility continuity checks will be conducted by the TCF and PTF to ensure compliance with work orders. The circuit is to be installed as indicated on the TSO and properly documented on the DD Form 1441: Circuit Data Card, and on any local equipment assignment or wiring records.

C8.3.2 Alignment. Performance of circuit alignment tests will be conducted by the TCF and PTF on in-facility circuitry and associated transmission links in conjunction with adjacent TCFs. Continuity and transmission level adjustments on the in-facility installation will be performed first. When the in-facility portion of the circuit is properly adjusted, the input and output levels on all external transmission channels assigned to the circuit must be adjusted to the proper value. Additional checks will be made, as required, to ensure proper functioning of conditioning and signaling equipment. When the internal and external alignments and checks are completed, an overall recheck of the complete installation will be made. In the specific cases where a PTF is located between the TCF and the user, the TCF is to ensure the transmission levels, signaling, and conditioning of the circuit are properly adjusted between the user

and the PTF. Notification will be made to the CCO or ICO that in-facility and adjacent link tests have been completed and meet required criteria. Participation in user-to-user testing will be conducted, as directed by the CCO.

C8.3.3 Testing. Each circuit installed in the GIG will be tested in accordance with the criteria specified in the GIG technical schedule for the type of circuit (circuit parameter code) in the TSO or Status Acquisition Message (SAM), as applicable. Upon notification from all intermediate TCFs that in-facility and adjacent segment tests are complete, the TCF designated as the CCO will initiate end-to-end tests of the circuit. All the specific test procedures required for ensuring compliance with the GIG circuit technical schedule parameters are shown in Supplement 1 to this Circular (reference 4.8).

C.8.3.1 The TCF and PTFs concerned will immediately notify the CCO or the ICO when, for any reason, delays are encountered or anticipated in activation of circuits. The notification will contain detailed information on reasons for delay or inability to activate circuits. Pertinent recommendations on methods of providing service should also be included.

C.8.3.2 Within 72 hours of notifying the CCO of delays, the facility not able to provide service, as specified by the TSO, will provide the originator and all addressees of the TSO, all pertinent information which precludes activation of TSO specified service. The CCO may use this information in the preparation of a delayed service report which should be submitted immediately.

C8.3.4 Certification. Certified, programmed, or anticipated telecommunications requirements may be of such magnitude as to require expansion of government-owned GIG facilities. DISA action agency commanders will monitor the use of facilities, correlate requirements to availability of facilities, and, when necessary, submit a subsystem project plan to the Director, DISA, who will obtain the necessary approvals and concurrences and forward the plan, with further implementing instructions, as necessary, to the appropriate military department (MILDEP) for action.

C8.3.5 Deactivation. Deactivation of circuits will be accomplished in accordance with TSO directions.

C8.4 Completion Reports. A completion report (CRP) is required for every TSO issued, unless specified differently in the TSO. (The in-effect report and DMS action notice submitted by DMS in accordance with DISAC 310-D70-30, Global Information Grid (GIG) National Gateway Center (NGC) and Subscriber Operations (reference 4.10), constitutes an in-effect report, and no separate report, as stated in this Circular, is required.) Completion reports shall not be required for a TSO which address administrative information only (e.g., telephone numbers, office symbol corrections, etc.). In the case of a Telecommunications Service Request (TSR) for leased equipment or services where a TSO is not issued, completion reports will be submitted unless specified differently in the TSR. In-effect reports for a Precedence Access Threshold (PAT) will be based upon Switch Revision Messages (SRMs) for outside continental United States (OCONUS) service and upon a PAT Telecommunications Request (TR) for continental United States (CONUS) service. The report informs the office that issued the order that action has been completed or that additional action may be required. Four different reports have been devised to cover all situations. The reports are designed to be processed by computer insofar as possible; therefore, the formats must be followed precisely. The types of reports are covered in detail in subparagraph C8.4.3.

C8.4.1 Submission. Completion reports will be submitted via DISA direct order entry (DDOE) (when available) or e-mailed directly to the originator of the TSO and all addressees on the TSO. Only one type of report should be included in any one message; i.e., do not submit an in-effect report and exception report in the same message. Completion reports for a Defense Switched Network (DSN) PAT TSR will be submitted and formatted in accordance with the examples shown in Supplement 1 to this Circular (reference 4.8).

C8.4.2 Format. Addressing the reports to the DMS or e-mail address of the appropriate DISA activity will help to ensure the reports are correctly routed for further processing. The addresses are as follows: PROVHQS@DISA.MIL, PROV PAC@DISA.MIL, PROVTMS@DISA.MIL, and PROVEUR@DISA.MIL. These e-mail addresses are for provisioning documents only (Telecommunication Service Request (TSR), delayed service report (DSR), in-effect report (IER), etc). Administrative type messages should not be sent to DISA or to the account manager using these addresses.

C8.4.3 **Types.** The types of completion reports are detailed as follows:

C8.4.3.1 **In-effect Report (IER).** The facility or activity designated in the TSO (normally the CCO or CMO) will, within 72 duty hours (based on 24-hour workday not including weekends and holidays) of completion of action on the TSO, forward an IER directly to the originator and all addressees of the TSO. If the service being in-effected has been assigned a TSP, the IER, containing the applicable TSP Authorization Code, must be submitted to tsp@dhs.gov. This report will be submitted either when the service is provided end-to-end and accepted, meets all details of the TSO, and meets all technical parameters of the specified technical schedule or to clear previously submitted exception or delayed service reports. One service will be covered by one IER. An example of an IER is shown in figure F8.2. An IER will contain the following information:

C8.4.3.1.1 Subject: In-Effect Report.

C8.4.3.1.2 Reference: Identification of the message forwarding the TSO.

C8.4.3.1.3 Item 1: Complete TSO number.

C8.4.3.1.4 Item 2: TR number from TSO paragraph 2N.

C8.4.3.1.5 Item 3: CCSD or trunk ID from TSO paragraph 2A.

C8.4.3.1.6 Item 4: Commercial carrier and commercial circuit number from TSO paragraph 3X2A or other sources, or enter NA.

C8.4.3.1.7 Item 5: Type action from TSO paragraph 2C.

C8.4.3.1.8 Item 6A: Date, time, month, and year of completion of action.

C8.4.3.1.9 Item 6B: Date, time, month, and year commercial service was provided, or enter NA when no commercial service has been requested.

C8.4.3.1.10 Item 7: Remarks. Note any administrative comments or minor changes authorized under chapter 2, subparagraphs 7.2.2 and 7.2.3 of DISAC 310-130-1 (reference 4.6).

C8.4.3.1.11 Item 8: Point of contact. Name, organization, and DSN commercial telephone number of person submitting the in-effect report.

C8.4.3.1.12 Item 9: NCS assigned TSP Authorization Code from item 102 of the TR and subparagraph 7.2.2 of the TSO.

C8.4.3.2 Exception Report. The facility or activity designated in the TSO (normally the CCO or CMO) will, within 72 duty hours (based on 24-hour workday not including weekends and holidays) of completion of action on the TSO, submit an exception report if end-to-end service is provided and accepted with some exceptions to, or deviations from, the details of the TSO or technical parameters of the specified technical schedule. Prior to accepting service, the designated facility or activity will advise the TSO issuing authority of those technical parameters failing to meet established standards, who will in turn advise the facility or activity if service is to be accepted with these exceptions. Exception reports will be forwarded directly to the originator and all addressees of the TSO. Follow-up reports will be submitted every 30 days until the exception(s) is cleared. If a firm date is known when the exception(s) will be cleared (e.g., equipment on order) and that information is contained in the followup, then subsequent followups are not required until the firm date indicated. All exception reports must be followed by an IER when the exceptions are cleared. An example of an exception report is shown in figure F8.3. Exception reports will contain the following information:

C8.4.3.2.1 Subject: Exception.

C8.4.3.2.2 Reference: Identification of the message forwarding the TSO.

C8.4.3.2.3 Item 1: Complete TSO number.

C8.4.3.2.4 Item 2: TR number from TSO paragraph 2N.

C8.4.3.2.5 Item 3: CCSD or trunk ID from TSO paragraph 2A.

C8.4.3.2.6 Item 4: Commercial carrier and commercial circuit number from TSO paragraph 3X2A or other sources or enter NA.

C8.4.3.2.7 Item 5: Type action from TSO paragraph 2C.

C8.4.3.2.8 Item 6A: Date, time, month, and year of completion of action.

C8.4.3.2.9 Item 6B: Date, time, month, and year commercial service was provided or enter N/A when no commercial service has been requested.

C8.4.3.2.10 Item 7: Exception code from chapter 20 of DISAC 310-65-1 (reference 4.9).

C8.4.3.2.11 Item 8: Rationale (mandatory). Enter narrative remarks to include which items are not as specified in the TSO; reason allocated channel was changed; a statement of which parameters could not be met with actual readings compared to required readings; identification of the authority or activity that authorized acceptance of substandard service; statement of which specifications could not be measured with reason and location; lack of response by a commercial carrier by name and location; proposed corrective action, if any, with estimated date and time for completion of corrective action; and any other remarks which will explain the exceptions.

C8.4.3.2.12 Item 9: Point of contact. Name, organization, and DSN and commercial telephone number of person submitting the exception report.

C8.4.3.3 Delayed Service Report (DSR).

C8.4.3.3.1 If leasing services are involved, refer to chapter 10.

C8.4.3.3.1.1 The facility or activity designated in the TSO to report on or accept the circuit will contact the local sales office of the vendor providing the service 5 working days prior to the scheduled service date to ascertain that the service date will be met.

C8.4.3.3.1.2 If the commercial vendor indicates the service date cannot be met due to vendor difficulties, a DSR will be telephoned to Defense Information Technology Contracting Organization (DITCO) and the requestor by the facility or activity designated in the TSO to report on or accept the circuit. The requestor will telephonically advise DITCO or the appropriate DITCO field activity. The verbal report will be confirmed by delayed service message to the requestor and to the originator and all addressees of the TSO within 72 hours.

C8.4.3.3.1.3 If the established service date cannot be met due to governmental causes, a DSR will be transmitted by the CCO or TR or TSO designated activity for reporting on or

accepting the circuit. This report will be sent to the requestor and to the originator and all addressees of the TSO, as soon as the inability to meet the required service date is known. When possible, this message report should be preceded by a verbal notification to the requestor who can issue an amended TR reflecting the new or revised required service date.

C8.4.3.3.2 If leased services are not involved, refer to chapter 8.

C8.4.3.3.2.1 When the established service date cannot be met due to governmental cause, the CCO or the TR and TSO designated activity for reporting on or accepting the circuit will submit a delayed service report. This report will be sent to the requestor, the originator, and all addressees of the TSO. It will be sent as soon as the inability to meet the required service date becomes known. When possible, this message report should be preceded by a verbal notification to the requestor.

C8.4.3.3.2.2 If the forecasted delay, as reported in item 8 of the delayed service report, is excessive (e.g., unknown), a report will be submitted each 30 days until a firm date is established. The problem may be resolved by exceptional procedures as outlined in subparagraph 2.4.2 of chapter 2 of DISAC 310-130-1 (reference 4.6).

C8.4.3.3.2.3 A DSR must always be followed by either an IER or an exception report.

C8.4.3.3.2.4 An example of a delayed service report is shown in figure F8.4. Delayed service reports will contain the following information:

C8.4.3.3.2.4.1 Subject: Delayed Service Report.

C8.4.3.3.2.4.2 Reference: Identification of the message forwarding the TSO.

C8.4.3.3.2.4.3 Item 1: Complete TSO number.

C8.4.3.3.2.4.4 Item 2: TR number from TSO paragraph 2N.

C8.4.3.3.2.4.5 Item 3: CCSD or trunk ID from TSO paragraph 2A.

C8.4.3.3.2.4.6 Item 4: Commercial carrier and commercial circuit number from TSO paragraph 3X2A or other sources, or enter NA.

C8.4.3.3.2.4.7 Item 5: Type action from TSO paragraph 2C.

C8.4.3.3.2.4.8 Item 6A: Date, time, month, and year specified in TSO paragraph 2D.

C8.4.3.3.2.4.9 Item 6B: Date, time, month, and year commercial service was provided or enter NA when no commercial service has been requested. This information is required even if the service, end-to-end, is not established. This information will be used by DITCO for billing purposes when a leased service is provided or accepted and the U.S. Government is obligated for payment and by the requestor or TSO preparing office to determine whether or not the leased service should be discontinued and restarted at a later date. Every effort must be made to amend TR and TSO service dates to preclude unnecessary expenditures. (See subparagraph C2.10.4.3.1.3 of DISAC 310-130-1 (reference 4.6) for additional details on completion reports.)

C8.4.3.3.2.4.10 Item 7: Delayed service code from chapter 20 of DISAC 310-65-1 (reference 4.9).

C8.4.3.3.2.4.11 Item 8: Date, time, month, and year service is expected to be provided or leave blank or enter 30 days from current date.

C8.4.3.3.2.4.12 Item 9: Cause (mandatory). If the delay is attributable to a commercial carrier, enter the reason for delay provided by the carrier and the name of the company; if user equipment or facilities are not installed or capable of operation, so state and enter any other amplifying remarks which will explain the delay.

C8.4.3.3.2.4.13 Item 10: Point of contact (POC). Name, organization, and DSN or commercial telephone number of person submitting the delayed service report.

C8.4.3.4 **Ready for Use Report (RFU)**. In instances where one or more DISA common user system(s) (PROMINA, Router, etc.) or commercial point-to-point circuits are installed, tested, and accepted by the government to satisfy a customer service requirement, an RFU will be issued. When all installation testing and acceptance (T&A) actions are satisfied (circuit and or equipment performance meets standards), the DISN circuit implementers (in coordination with the customer and or the CCO and CMO) will submit the RFU report to the applicable

provisioning activity and provide information copies to all order addressees. The RFU must be followed by an in-effect report issued by the CCO and CMO when the end-to-end service is installed. An example of an RFU is shown in figure F8.5. An RFU will contain the following:

C8.4.3.4.1 Reference: TSO Document.

C8.4.3.3.2 Item 1: Complete TSO number.

C8.4.3.3.3 Item 2: TR number from TSO paragraph 2N.

C8.4.3.3.4 Item 3: CCSD or trunk ID from TSO paragraph 2A.

C8.4.3.3.5 Item 4: Commercial carrier and commercial circuit number from TSO paragraph 3X2A or other sources, or enter N/A.

C8.4.3.3.6 Item 5: Type action from TSO paragraph 2C.

C8.4.3.3.7 Item 6A: Date, time, month, and year of completion of action.

C8.4.3.3.8 Item 6B: Date, time, month, and year commercial service was provided, or enter NA when no commercial service has been requested.

C8.4.3.3.9 Item 7: Remarks. (i.e., Amplifying remarks relative to circuit being ready for use.)

C8.4.3.3.10 Item 8: Point of contact (POC). Name, organization, and DSN and commercial telephone number of person submitting the RFU report.

C8.4.3.3.11 Item 9: CCO and CMO POC and phone number.

Return to:

Chapter 6

[Basic Circular](#)

[Top of Table of Contents](#)

[DISA Publication Listing](#)

[DISA Home Page](#)

Continue to:

Chapter 9

DISA PUBS@DISA.MIL - Last change: 21 March 2012

FIGURE F8.1 SAMPLE TELECOMMUNICATIONS SERVICE ORDER (TSO)

ZEN CMO.USAFE@SCOTT.AF.MIL
ZEN DISACKTATIONSEURUC@DISA.MIL
ZEN DISAEUR.PATCHANDTEST@DISA.MIL
ZEN DISN-EUR@DISA.MIL
ZEN DISNNE@DISA.MIL
ZEN DITCOATD@DISA.MIL
ZEN DL5THCM@EUR.ARMY.MIL
ZEN DL5THG3-P&E-TSO@EUR.ARMY.MIL
ZEN DL5THG3-RFS@EUR.ARMY.MIL
ZEN DRSN@39SIGBN.ARMY.MIL
ZEN GSIO@DISA.MIL
ZEN IP-ANALYSTS@DISA.MIL
ZEN PAWS@PAWS.CSD.DISA.MIL
ZEN PL511@DISA.MIL
INFO ZEN CMO.USAFE@SCOTT.AF.MIL
ZEN TSP@DHS.GOV
ZEN CIRCUIT.ACTIONS@RAMSTEIN.AF.MIL
ZEN CSS.SCBS@RAMSTEIN.AF.MIL
ZEN CMO.USAFE@SCOTT.AF.MIL
ZEN CIRCUITS@AFNOC.AF.MIL
ZEN 754ELSG.DOOA@GUNTER.AF.MIL
ZEN AFNOC.NOD.CIRCUITACTIONS@GUNTER.AF.MIL
ZEN AFLHCIRCUITS@GUNTER.AF.MIL
ZEN DCSSTA@EUR.ARMY.MIL
ZEN DRSN@EUR.ARMY.MIL
ZEN 703MUMSS.CA635776@VOLKEL.SPANGDAHLEM.AF.MIL
ZEN TCROSS@SCOTT.AF.MIL

BT

UNCLAS

SUBJ: TSO E80987/MSB0-01 //SOONER IF POSSIBLE//

REF: CMO.USAFE@SCOTT.AF.MIL// DTG 121253Z SEP 12 TSR BF05MAY125088.

1. PURPOSE

- A. THIS TSO IS ISSUED TO START A 1.984MB, X.21 SIPRNET CIRCUIT BETWEEN VOLKEL, NL AND SHAPE CASTEAU, BE.

703MUNNS IS REQUIRED TO UPDATE THIER SIPRNET ACCREDICATION PACKAGE TO SHOW UPGRADE OF SPEED OF CIRCUIT.

REQUEST THAT DISA SCAO APPROVE THE EXISTING ACCREDICATION PACKAGE OF CIRCUIT MOPP FOR CIRCUIT ACTIVATION UNTIL 703MUNS CAN SUBMIT UPGRADE PACKAGE THROUGH COMMAND AND AF FOR APPROVAL.

- D. FOR DITCO: PLEASE TAKE ACTION TO START A 1.948MB, X.21 CONNECTION BETWEEN VOLKEL, NL AND SHAPE CASTEAU, BE. THE VENDOR IS REQUIRED TO PROVIDE TIMING.

2. GENERAL CIRCUIT/TRUNK INFORMATION

- A. JS79MSB0 B. NA C. START
D. 010800Z AUG 11
E. (1) VOLKEL SPH NL/4 CONTACT: (PMRY POC) SSGT THOMAS DOE; (ORG) 703MUNSS.CA635776@VOLKEL.SPANGDAHLEM.AF.MIL; (USER) THOMAS.DOE@VOLKEL.SPANGDAHLEM.AF.MIL; (CMCL) 00-31-1433-35916; (DSN) 314-359-5916; (ALT POC) SSGT FRANK DOE; (USER) JOHN.DOE@VOLKEL.SPANGDAHLEM.AF.MIL; (CMCL) 00-314-1333

FIGURE F8.1 SAMPLE TELECOMMUNICATIONS SERVICE ORDER (CONTINUED)

(2) SHAPECST SP1 BE/4 CONTACT: SUPERVISOR, D314-366-6220/6209,
 C32-6532-6220/6209; EMAIL: DRSN@EUR.ARMY.MIL
 F. Y1 4G G. FULL DUPLEX
 H. CCO SHAPECST/BE/TCG/D314-366-6199,C0032-6532-61
 I. 1.984MB J. UNSECURE K. FULL PERIOD
 L. NO SIGNALING
 M. NA N. BF05MAY115088 O. NA P. A Q. A
 R. 1UXXGS S. DF T. NA
 U. (1) N/A
 (2) N/A
 (3) N/A
 X. NA AA. NA AB. CCI AC. NA
 AD. NA AE. NA AF. NA AG. NA AH. NA
 AI. NA AJ. NA AK. NA
 AL. NA AM. NA AN. NA
 AO. NA AP. NA AQ. NA AR. NA AS. NA AT. NA
 AU. NA AV. NA AW. NA AX. NA

3. FACILITY AND EQUIPMENT INFORMATION

A. VOLKEL NL4SPH
 BLDG/DIRECTIONS/ADDRESS: VIB VOLKEL 404
 RM/FL: 4; GND FL
 CONTACT: (PMRY POC) SSGT THOMAS DOE; (ORG)
 703MUNSS.CA635776@VOLKEL.SPANGDAHLEM.AF.MIL; (USER)
 THOMAS.DOE@VOLKEL.SPANGDAHLEM.AF.MIL; (CMCL)
 00-31-1433-35916; (DSN) 314-359-5916; (ALT POC) SSGT
 JOHN.DOE; (USER)
 JOHN.DOE@VOLKEL.SPANGDAHLEM.AF.MIL; (CMCL)
 00-314-1333-5916; (DSN) 314-359-5916
 MAIL ADDRESS: 703 MUNSS/SCB
 UNIT 6790
 APO, AE 09717-5018
 DEMARK: 703 MUNSS/SCB, BLDG 404, RM 4, ZEELANSEDIJK 10, 5408 SM
 VOLKEL AB
 UNIT ID: USAF/USAFE
 (1) (A) CISCO 4500 ROUTER;
 INTERFACE: SERIAL
 IP ADDRESS: 140.50.141.14
 SUBNET MASK: 255.255.255.252
 (B) CABLE CROSS CONNECT
 (C) KIV-19
 (D) CABLE CROSS CONNECT
 (E) INTERFACE: GFE ADAPTER, X.21 TO RS-530/RS-449
 EXTERNAL CLOCK PROVIDED BY VENDOR PTT PROVIDED CSU/DSU;
 (PHYSICAL) DB25; (ELECTRICAL) B8ZS/ESF
 (F) INTERFACE: PTT PROVIDED CSU/DSU X.21 SERVICE; (PHYSICAL)
 X.21
 (G) COMMERCIAL DISTRIBUTION FRAME
 (2) (A) 44 L NO SIG UNKN UNKNOWN D 1UXXGS
 (H) 140.50.141.14

FIGURE F8.1 SAMPLE TELECOMMUNICATIONS SERVICE ORDER (CONTINUED)

B. SHAPECST BE4TCG

BLDG/DIRECTIONS/ADDRESS: 185

RM/FL: 204A

CONTACT: SUPERVISOR, 314-366-6199/6353; EMAIL:

DCSSTA@EUR.ARMY.MIL

MAIL ADDRESS: SHAPE GIG

UNIT 21419

APO AE 09708

DEMARK: (BLDG) 185; (RM) 240 A; SHAPE DRSN FACILITY; 39TH SIGNAL
BATTALION; UNIT 21420; AVE DU BERLIN; 7010 SHAPE

BELGIUM

UNIT ID: USA/USAREUR

- (1) (A) COMMERCIAL DISTRIBUTION FRAME
- (B) INTERFACE: PTT PROVIDED CSU/DSU X.21 SERVICE; (PHYSICAL)
X.21
- (C) INTERFACE:
TERM: 8W
INTERFACE: GFE ADAPTER, X.21 TO RS-530/RS-449
EXTERNAL CLOCK PROVIDED BY VENDOR PTT PROVIDED CSU/DSU;
(PHYSICAL) DB25; (ELECTRICAL) B8ZS/ESF
- (D) CANOGA PERKINS FIBER MODEM
- (E) COMMERCIAL DISTRIBUTION FRAME
- (2) (A) 44 C NO SIG Z

C. SHAPECST BE4SP1

BLDG/DIRECTIONS/ADDRESS: 101

RM/FL: J-101

CONTACT: SUPERVISOR, D314-366-6220/6209, C32-6532-6220/6209;

EMAIL: DRSN@EUR.ARMY.MIL

MAIL ADDRESS: SHAPE DRSN FACILITY

39TH SIGNAL BATTALION

UNIT 21420

APO AE 09705

DEMARK: BLDG 185, RM A204, AVE DU BERLIN, 7010 SHAPE BELGIUM

UNIT ID: USA/USAREUR

- (1) (A) CANOGA PERKINS FIBER MODEM
- (B) CABLE CROSS CONNECT
- (C) KIV-19
- (D) CABLE CROSS CONNECT
- (E) CISCO ROUTER 7204
NODE ID: CCEESHM010
IP ADDRESS: 140.50.141.13
SUBNET MASK: 255.255.255.252
INTERFACE: SE3/2
- (2) (H) 140.50.141.13

4. NUMBER CONTROL

A. N/A

B. N/A

C. N/A

5. OTHER SPECIFIC DIRECTIONS

A. OPERATIONAL SERVICE DATE: 010800Z AUG 12(SIP)

B. COMMERCIAL/GFE DATE: 010800Z AUG 12(SIP)

C. NETWORK SVC: SIPRNET

D. SVC APPLIES TO: CIRCUIT ONLY/SINGLE VENDOR

FIGURE F8.1 SAMPLE TELECOMMUNICATIONS SERVICE ORDER (CONTINUED)

- E. CCCI/CSA: NEW LEASE
- F. TSR CONTACT: USAF; USAFE; MR. BOB E DOE;
(ORG) CMO.USAFE@SCOTT.AF.MIL
(USER) BOBY.DOE.CTR@SCOTT.AF.MIL;
(CMCL) 001-618-207-2133
- G. NSS: Y3
- H. SEC RQMT ACCESS: (SP A) ESCORT REQUIRED; FOR SITE ACCESS, PLEASE CONTACT POC LISTED ABOVE. PTT MUST GIVE AT LEAST 48 HRS NOTIFICATION FOR ACCESS.
(SP B) ESCORT REQUIRED
- I. O/S SHIPPING INS: (** SHIPPING ADDR **)
(SP A) 703 MUNSS/SCB; UNIT 6790; APO, AE, 09717; (BLDG) VIB VOLKEL 404 (ZEELANDESDIJK; (RM) 5; (FL) GND
(SP B) SHAPE DRSN FACILITY; 39TH SIGNAL BATTALION UNIT 21420; APO, AE, 09705; (BLDG) 185; (RM) 240 A
(SP C) SHAPE DRSN FACILITY; 39TH SIGNAL BATTALION UNIT 21420; APO, AE, 09705; (BLDG) 101; (RM) J-101 J. COST THRESHOLD/DISN ESTIMATED COST: (NTE MRC) \$5200.00; (NTE NRC) \$3000.00
- K. REMARKS: ** ADDITIONAL INFORMATION PERTINENT TO THIS REQUIREMENT IS POSTED BELOW WITH RESPECTIVE LABELS **
(** DISA COST ESTIMATE **)
DESCRIPTION: TRANSMISSION SERVICES
BILLING BANDWIDTH: 1.984MB; MRC: \$5200.00; NRC: \$3000.00;
TOTAL DISA COST ESTIMATE: MRC: \$5200.00; NRC: \$3000.00;
NOTICE: DISA COST ESTIMATE IS SUBJECT TO CHANGE. ANY CHANGE IN THE COST ESTIMATE (MRC/NRC) WILL BE COORDINATED WITH THE AGENCY REQUESTING THE SERVICE PRIOR TO DISA FINALIZING THE REQUIREMENT.
DISCLAIMER: IF YOU CHANGE THE TYPE OF SERVICE, BANDWIDTH, OR SERVICE POINTS (GEOLOC CODE), THEN THE TR IS REROUTED TO THE DISA ENGINEERING OFFICE.; COST ESTIMATE DOES NOT INCLUDE THE 1.25% FEE-FOR-SERVICE CHARGE.;
(** AFO **) ROBERT E DOE; (ORG) CMO.USAFE@SCOTT.AF.MIL;
(CMCL) 001-618-207-2133; PATTY DOE; (ORG) AFCA.ECLF@SCOTT.AF.MIL; (CMCL) 618-229-6190; (DSN) 779-6190
(** GEO DISPOSITION **) EUR (AREAS 3,4,5,6)
(** REMARKS **)
1. PER CONVERSATION WITH MR. JOSHUA HAWKINS/DISA EUROPE, MS CARMA-LYNN POLLOCK/AFCA AND MR. JAMES DENNIS/USAFE CMO. PRESENT SIPRNET CIRCUIT MOMP IS A 128KB X.21 SERVICE ON TWO SEPERATE LEASES. TOTAL LEASE COST FOR 128KB CIRCUIT IS OVER \$5000 IN MRC CHARGES. NEW CIRCUIT WILL UPGRADE SERVICE FOR SAME PRICE.
 2. ON ACTIVATION OF THIS SERVICE USAFE CMO WILL INITIATE SEPERATE CHANGE TR TO DISCONTINUE CIRCUIT MOMP AND EXISTING CSA'S DB W 262468 AND NPPT W 262468 BETWEEN RAMSTEIN, GE AND VOLKEL, NL.
 3. USER LOCATION HAS BEEN APPROVED BY AFSN PROJECT ENGINEERS. ENGINEERING POC IS MR. PAT WALTERS, DSN 596-6480; WALLACE.WALTERS@GUNTER.AF.MIL
 4. AFSN NUMBER: AFSN08006022
 5. USER DESIRES AND WILL ACCEPT EARLIEST POSSIBLE SERVICE DATE.
(** DISA MANAGED ROUTER **) NO
(** COMSEC INFO CONT'D **) (SP A) (DSN) 314-359-5916; (USER)

FIGURE F8.1 SAMPLE TELECOMMUNICATIONS SERVICE ORDER (CONTINUED)

- L. REMARKS CONTINUED: JEFF.ROY@VOLKEL.SPANGDAHLEM.AF.MIL
(** DEMARC CONT'D **) (SP C) (PMRY DEMARC POC) MR. RAYMOND E
SCHRAEDER;
(ORG) DRSN@BENELUX.ARMY.MIL; (USER)
RAYMOND.SCHRAEDER@BENELUX.ARMY.MIL; (CMCL) 011-32-06544-6027;
(DSN) 314-366-6027
- M. EST SVC LIFE: 60 MONTHS
- N. RFS NO: WO15JAN088314
- O. REPORTING: STATION DESIGNATED IN PARAGRAPH 2H AS CCO/CMO WILL
SUBMIT COMPLETION REPORT IAW DISAC 310-130-1, SUPP 1, 2, 3 FORMAT
OR DISAC 310-70-1. REPORT WILL BE ADDRESSED TO ORIGINATOR AND
ALL ADDRESSEES OF THIS TSO.
- P. T&A IS REQUIRED. CIRCUIT WILL BE TESTED IAW ESTABLISHED TEST
SCHEDULES IN DISAC 310-70-1. TEST RESULTS WILL BE MAINTAINED IN
THE CIRCUIT HISTORY FOLDER AT SERVING TECH CONTROLS. TEST RESULTS
WILL NOT BE SUBMITTED TO HIGHER ACTIVITIES UNLESS SPECIFICALLY
REQUESTED.
- Q. SIPR/NIPR, PROMINA, ATM CIRCUITS AND TRUNKS, ITSDN SERVERS, AND
XTACACS SERVERS ARE WAIVERED FROM PERIODIC OUT OF SERVICE (OOS)
QUALITY CONTROL (QC) TESTING.
- R. EUROPEAN INTERNET PROTOCOL ROUTER PROVISIONING REQUIREMENT.
(DISNNE@NCR.DISA.MIL) PLEASE TAKE ACTION TO PLACE THIS
REQUIREMENT ON THE MASTER SCHEDULE WITH THE INSTALLATION DATE
LISTED IN 2D. ANY CHANGES TO THIS DATE WILL BE SUBMITTED VIA
EMAIL. INSTALLATION AND ACTIVATION OF THIS CONNECTION IS
CONTINGENT UPON RECEIPT AND ACCEPTABLE REVIEW OF SIPRNET SECURITY
PACKAGE (SSP) AND SUBSEQUENT CONNECTION APPROVAL FROM DISA
HEADQUARTERS - D25. USER MUST INSURE THAT SSP INFORMATION IS
CURRENT AT ALL TIMES. QUESTIONS CONCERNING SIPRNET CONNECTION
APPROVAL PROCESS MAY DIRECTED TO DISA EUROPE DATA IMPLEMENTATIONS
- EU51, DSN: 434-5457.
- S. TSO CONTACT: MICHAEL T. PACE, EU8, DSN: 434-5072; CML:
0711-68639-5072; EMAIL: john.doe@disa.mil
6. DDN/DISN SERVICE INFORMATION
- | | | | |
|---|---|--|---------------|
| A. NA | B. NA | C. NA | D. UNASSIGNED |
| E. UNASSIGNED | F. NA | | G. UNASSIGNED |
| H. NA | | | |
| I. NA | | | |
| J. NA | K. UNASSIGNED | L. CA635776 | |
| M. SSGT THOMAS DOE; (CMCL) 00-31-1433-35916 | N. 703 MUNNS/CA635776; UNIT 6790; APO, AE, 09717 | O. (ORG) 703MUMSS.CA635776@VOLKEL.SPANGDAHLEM.AF.MIL | |
| P. UNASSIGNED | NA | | |
- BT

Return to:

Chapter 6

[Basic Circular](#)

[Top of Table of Contents](#)

[DISA Publication Listing](#)

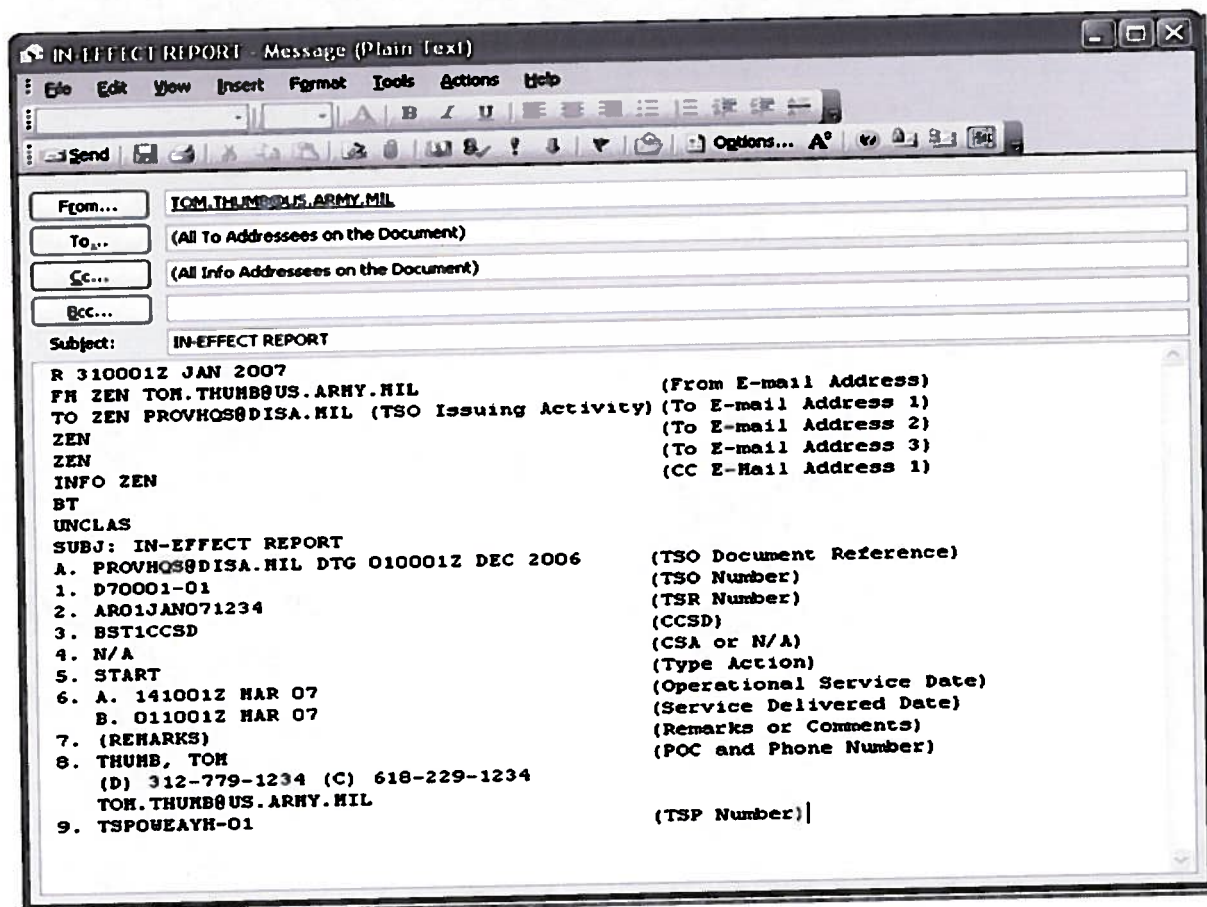
[DISA Home Page](#)

Continue to:

Chapter 9

DISA Pubs@DISA.MIL - Last change: 21 March 2012

FIGURE F8.2 Sample In-Effect Report (IER)



Return to:

Chapter 6

[Basic Circular](#)

[Top of Table of Contents](#)

[DISA Publication Listing](#)

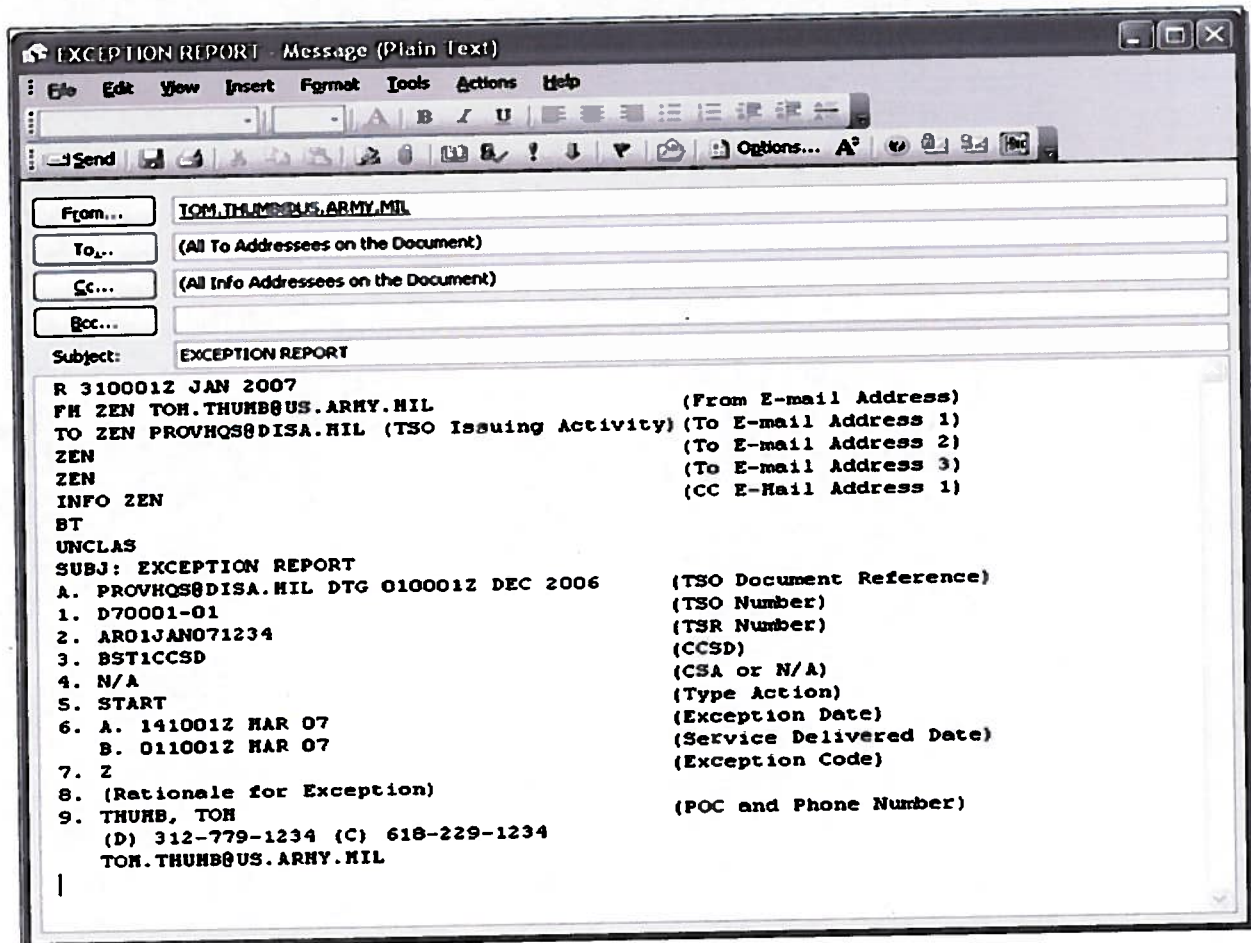
[DISA Home Page](#)

Continue to:

Chapter 9

DISA PUBS@DISA.MIL - Last change: 21 March 2012

FIGURE F8.3 Sample Exception Report



Return to:

Chapter 6

[Basic Circular](#)

[Top of Table of Contents](#)

[DISA Publication Listing](#)

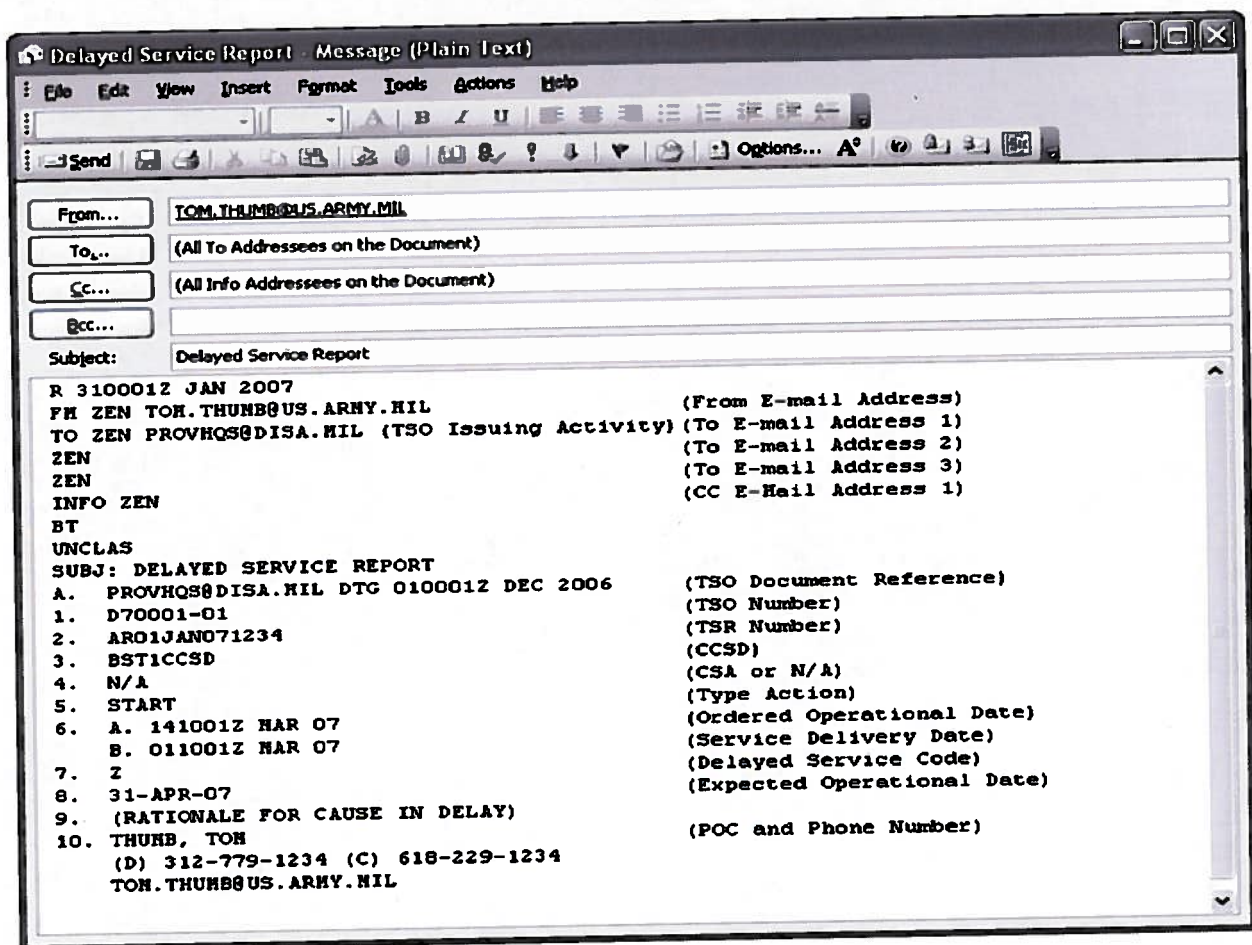
[DISA Home Page](#)

Continue to:

Chapter 9

DISA PUBLS@DISA.MIL - Last change: 21 March 2012

FIGURE F8.4 Sample Delayed Service Report (DSR)



Return to:

Chapter 6

[Basic Circular](#)

[Top of Table of Contents](#)

[DISA Publication Listing](#)

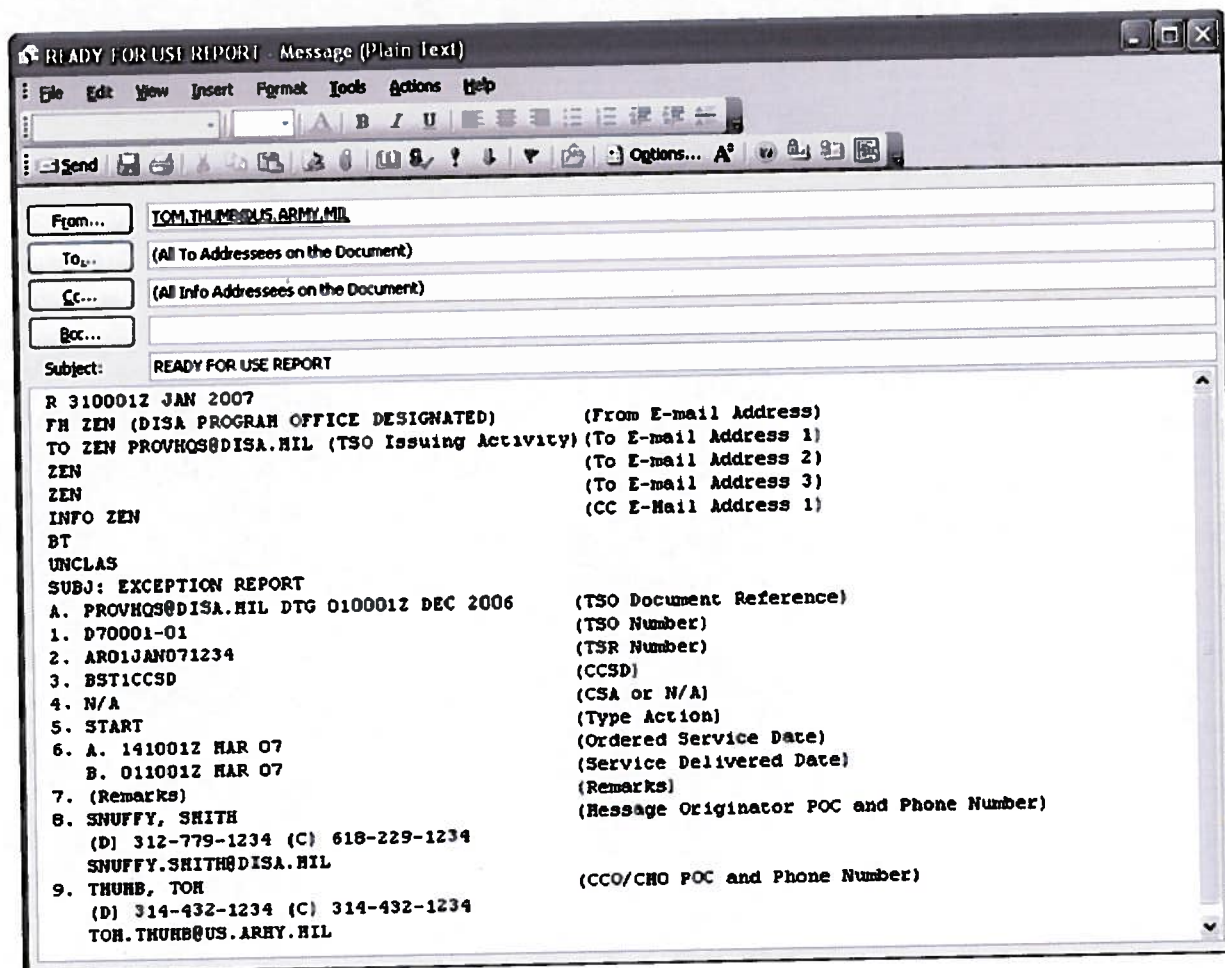
[DISA Home Page](#)

Continue to:

Chapter 9

DISA Pubs@DISA.MIL - Last change: 21 March 2012

FIGURE F8.5 Ready For Use (RFU) Report



Return to:

Chapter 6

[Basic Circular](#)

[Top of Table of Contents](#)

[DISA Publication Listing](#)

[DISA Home Page](#)

Continue to:

Chapter 9

DISA PUBS@DISA.MIL - Last change: 21 March 2012

C9. CHAPTER 9. ADMINISTRATION

C9.1 **General.** This chapter prescribes the various forms, logs, and publications required by each manned Global Information Grid (GIG) facility. Automated, electronic soft copy records, forms, and logs are authorized as specified in paragraph C9.2. When the facility is appropriately equipped, it can potentially have a fully automated circuit history folder, e.g., Telecommunications Service Order (TSO), applicable associated Department of Defense (DD) Forms, Circuit Layout Records (CLR), applicable reports, and any circuit specific information deemed relevant. If history files are lost or destroyed, a Technical Control Facility (TCF) and Patch and Test Facility (PTF) are required to obtain the latest TSO that reflects the current end-to-end circuit configuration. A copy of the latest TSO should be obtained by accessing the World Wide Online System (WWOLS) or Telecommunications Certification Office Support System (TCOSS) or by contacting adjacent TCF and PTFs in the circuit routing, the area facility control office (FCO), the requestor, and, as a last resort, the DISA TSO issuing authority. The prescribed forms are necessary for maintaining complete operational status of GIG facilities, links, trunks, circuits, and equipment. Upon completion, the forms also provide significant historical data that can be used to identify and correct recurring problems or problems that may require higher level assistance. The number and type of forms used in a GIG facility may vary somewhat with each facility, depending on that facility's particular mission. Each operation and maintenance (O&M) agency is to produce and distribute the forms to subordinate units. The forms prescribed by this Circular are listed below and are available on the Internet at the Department of Defense Management Forms Page located at <http://www.dtic.mil/whs/directives/informat/forms/>.

C9.1.1 DD Form 1441: Circuit Data

C9.1.2 DD Form 1443: Outage and Restoration Record

C9.1.3 DD Form 1697: Circuit Parameter Test Data - Analog

C9.1.4 DD Form 1697-1: Circuit Parameter Test Data - Digital

C9.1.5 DD Form 1753: Master Station Log

C9.2 Automated Recordkeeping. Automated recordkeeping using automated data processing (ADP) hardware and software is encouraged as it enhances efficiency and analysis capabilities, especially when integrated with other requirements contained in this Circular. O&M agencies responsible for operating and maintaining GIG facilities may develop application software to automate and integrate the requirements of the forms cited in subparagraphs C9.1.1 through C9.1.5 with other DISA requirements; such as, testing, trend analysis, circuit history folders TSOs, completion reports, circuit layout records, etc. Records can be inputted and or manipulated through utilization of various automatic data processing (ADP) tools and enable the facility to import and input data as well as images. Scanned images, such as circuit layout records, test results etc., are also authorized. Application software may emulate the above forms and contain the same data, but cannot use the DD form number. The DoD Forms Management Office is the only authority for use of DoD form numbers. Application software must have sufficient capabilities to meet all DISA requirements and have approved life-cycle maintenance. DISA is not responsible for evaluating or approving application software. However, the application software program developed and maintained by the Air Force facility and circuit information tracking (FaCIT), is considered adequate and is highly recommended. Each GIG facility is to ensure the ADP system is engineered and configured in such a manner to provide efficient use and cover contingencies. When the below conditions for automated record keeping are met, the facility is not required to maintain physical hard copies of circuit records. In general, any ADP system for recordkeeping purposes must conform to the following guidelines:

C9.2.1 The ADP system must provide for adequate backup capability so that computer failure will not prevent the maintenance of required records or the retrieval of information. Data stored on magnetic media must be duplicated on backup media at least once each day to minimize the chance of loss. The backup process should be an automated procedure or should at least prompt the operator to perform the required actions.

C9.2.2 The ADP system must be redundant with a second computer immediately available to replace a failed unit. If this is not possible, a hard copy of all records stored in the ADP system must be manually retained on file for the same length of time as the form it replaces.

C9.2.3 If ADP systems are used to maintain TCF and PTF records, all personnel must also be trained to use the paper forms cited in subparagraphs C9.1.1 through C9.1.5. A 90-day supply of paper forms must be maintained and accessible to personnel on duty. Contingency procedures must be developed to include instructions on how and when to revert to manual recordkeeping.

C9.2.4 Detailed outage records, sufficient to reconstruct events during the outage, must be retained in memory a minimum of 90 days. After this time, the detailed information may be purged from the records, and the information necessary for long-term analysis retained. The minimum information required for long-term analysis is the circuit, trunk, link, or facility designator, the date and time out, the date and time in, the reason for outage (RFO) code and location, and a brief narrative RFO.

C9.3 Required Forms.

C9.3.1 **DD Form 1441: Circuit Data.** The purpose of the DD Form 1441 is to provide quick access to appropriate trunk and circuit engineering information such as end terminals, channel numbers, type circuit, modulation and data rates, etc. A DD Form 1441 is required for all trunks and circuits that have a physical patch panel appearance in the TCF and PTF and for all trunks and circuits for which the TCF and PTF is the Communications Control Office (CCO) and Communications Management Office (CMO) or servicing TCF and PTF. Information for preparing the circuit data form should be taken from the TSO as a primary source. In-house facility equipment and circuit appearances must be added as required. A DD Form 1441 should be filed alpha numerically by the command communications service designator (CCSD) and trunk designator for quick reference. A DD Form 1441 must be maintained in a "dead file" for 3 months after the circuit has been deactivated. The following procedures must be followed when completing the form.

C9.3.1.1 **CCSD.** Enter the CCSD from the TSO.

C9.3.1.2 **Landline Channel Number.** Enter multiplex trunk and channel number or cable designation for each direction from the TSO.

C9.3.1.3 **Terminals.** Enter user terminal facilities by geographical location (GEOLOC) and en route facility code from the TSO.

- C9.3.1.4 **Control Facilities.** Enter the GEOLOC of the TCFs adjacent to the user terminal location from the TSO.
- C9.3.1.5 **NCS TSP.** Enter the National Communications System (NCS) Telecommunications Service Priority (TSP) restoration priority from the TSO.
- C9.3.1.6 **Term Station.** Enter GEOLOC of each terminal facility from the TSO.
- C9.3.1.7 **Operating Agency.** Enter the O&M agency of each terminal facility, if known.
- C9.3.1.8 **User Term Equipment.** Enter type or model of user terminal equipment from the TSO.
- C9.3.1.9 **User Contact.** Enter user contacts from the TSO or as otherwise available.
- C9.3.1.10 **Type Circuit.** Enter circuit parameter code from the TSO.
- C9.3.1.11 **Use.** Enter Automatic Message Handling System (AMHS), Defense Switched Network (DSN), internet protocol (IP) router networks, etc.
- C9.3.1.12 **CCO.** Enter the CCO or CMO from the TSO.
- C9.3.1.13 **Modulation Rate.** Enter modulation rate from the TSO.
- C9.3.1.14 **Crypto Service.** Enter security equipment nomenclature from the TSO.
- C9.3.1.15 **Activation Authority.** Enter the TSO number.
- C9.3.1.16 **Date and Time Installed (Activated).** Enter the date and ZULU time shown in the in-effect report.
- C9.3.1.17 **Deactivation Authority.** Enter the TSO number discontinuing the circuit.
- C9.3.1.18 **Date and Time Ceased.** Enter date and ZULU time circuit discontinued.

C9.3.1.19 **CKT Modifications.** Enter the latest TSO number directing changes to the circuit, and date and ZULU time change completed.

C9.3.1.20 **Conditioning Equipment.** Enter conditioning and signaling equipment locations (rack number, jack number, strapping options etc.) for all in-facility equipment.

C9.3.1.21 **Remarks.** Enter circuit routing and trunk, link, and channel assignment of each facility from the TSO.

C9.3.1.22 **Bottom Line of Card.** The bottom line of the card must be completed, using the entries on the top line, when aKardex type file is used.

C9.3.1.23 **Reverse Side of Card.** The reverse side of the DD Form 1441 may be used for the purpose of the circuit layout record (CLR).

C9.3.2 **DD Form 1443: Outage and Restoration Record.** DD Form 1443 must be used to record all facility, link, trunk, circuit, channel, or equipment outages. The form provides a synopsis of the outage or degradation and a historical record for trending. Outage and restoration records must be maintained for 90 days after the end of each month. Detailed explanations of each entry are as follows:

C9.3.2.1 **Reportable.** Indicate if the outage is reportable to DISA and or to the Defense Information Technology Contracting Organization (DITCO) by circling the corresponding "YES" or "NO."

C9.3.2.2 **Ticket Number.** Indicate the ticket number assigned to the fault or outage report to which this form applies. A ticket number must be assigned by the control facility responsible for recording the outage. Ticket numbers will consist of the Julian date for the radio day (RADAY) the ticket was opened on and the sequential number for that RADAY (e.g., 158-001). If there is more than one control facility at the same location, it is permissible to precede or succeed the number by an alpha character to identify the specific facility.

C9.3.2.3 **Facility.** Indicate the facility designator for the send (SND) and receive (RCV) terminals of the link, trunk, circuit, channel, or equipment affected. (Leave blank for facility outage.)

C9.3.2.4 **Facility/Link/Trunk ID.** Indicate the applicable designator for the type of outage.

C9.3.2.5 **CHNL NBR.** Indicate the channel (CHNL) number (NBR) for circuit affected, if applicable.

C9.3.2.6 **CCSD/CSA.** Indicate the command communications service designator (CCSD) and/or communications service authorization (CSA) identifier for the circuit affected.

C9.3.2.7 **TSP.** Indicate the Telecommunications Service Priority (TSP) restoration priority code for the circuit affected. If no TSP is assigned, enter NA (Not Assigned).

C9.3.2.8 **Time Out.** Indicate the time that the outage began, in date time group (DTG) format (e.g., 111300Z JAN 12).

C9.3.2.9 **Time In.** Indicate the time that the outage was terminated, in date time group (DTG) format (e.g., 111300Z JAN 12).

C9.3.2.10 **RFO.** Indicate the Reason for Outage (RFO) for the associated Time Out and Time In entries.

C9.3.2.11 **Coordination.** Indicate the designator of the facilities or agencies coordinated with during the course of the outage under the "FAC" column. The "USER" and "TCF" coordination are already indicated. Other facilities or agencies can be documented in the blank blocks. Indicate the initials of the individual who was coordinated with at the other facilities or agencies during coordination of the "OUT" and "IN" times.

C9.3.2.12 **Reported Trouble.** Indicate the trouble, fault, discrepancy, or hazardous condition (HAZCON), as applicable to this ticket.

C9.3.2.13 **Equipment Nomenclature.** Used for work order information or as applicable for outages. Indicate the equipment nomenclature that is at fault or under repair.

C9.3.2.14 **Workorder Number.** Indicate the work order number assigned by maintenance for equipment under repair. For commercial carrier outages, this block can be used to document the commercial order or reference number.

C9.3.2.15 Maintenance Start. Indicate when maintenance repairs begin, in DTG format. For commercial carrier outages, this block is used to indicate when the outage was reported to the carrier. This is the beginning of the time chargeable to the carrier, in accordance with Defense Information Technology Contracting Organization (DITCO) procedures contained in DISA-DITCO Circular 350-135-1, Defense Commercial Communications Acquisition Procedures (reference 4.11).

C9.3.2.16 Equipment ID. Used to record the specific equipment identification, if a local equipment identification has been assigned.

C9.3.2.17 Maintenance Activity. Indicate the maintenance activity responsible for performing the repairs. For commercial carrier outages this block is used to identify the commercial activity responsible for the circuit.

C9.3.2.18 Maintenance End. Indicate when maintenance repairs are complete, in DTG format. For commercial carrier outages, this block is used to indicate when the commercial carrier turned control of the circuit back to the user for verification. This is the end of the time chargeable to the carrier, in accordance with DITCO procedures contained in DISA-DITCO Circular 350-135-1 (reference 4.11). If the circuit is unacceptable after the commercial carrier turns the circuit back, it must be reported back out to the carrier within 30 minutes in which case the outage time chargeable to the carrier will be continuous from the initial time it was reported to the carrier.

C9.3.2.19 Hazardous Condition. Indicate whether or not the "reported trouble" constitutes a hazardous condition (HAZCON), as prescribed in DISAC 310-55-1, Status Reporting (reference 4.1). Circle "YES" or "NO."

C9.3.2.20 ETR. Indicate the estimated time of return (ETR) for equipment under repair or HAZCON as applicable.

C9.3.2.21 Initials. Enter the initials of the maintenance individual who the problem was reported to and the initials of the maintenance individual who the corrective action was cleared with. If the problem is with a commercial carrier, this block is used to record the initials of the contractor's representative when the outage was reported out to the contractor and when the contractor turned it back upon completion of repairs.

C9.3.2.22 **Corrective Action.** Indicate the actual action taken to restore the service. Do not merely restate the RFO code.

C9.3.2.23 **Circuit Rerouted.** Indicate the CCSD or CSA of the circuit rerouted.

C9.3.2.24 **Patch Up.** Indicate the actual time, in DTG format, that the circuit was patched to the alternate route.

C9.3.2.25 **Patch Down.** Indicate the actual time, in DTG format, that the patch was removed.

C9.3.2.26 **Circuit Preempted.** Indicate the CCSD or CSA of the circuit being preempted. If a spare channel is used, indicate that it is spare.

C9.3.2.27 **Reroute Remarks.** Indicate any remarks that are pertinent to the reroute.

C9.3.2.28 **Supervisor's Review.** This block must be signed by the shift supervisor when commercial carrier outage is incurred.

C9.3.2.29 **Reverse Side, Date Time Group.** Indicate the time, in DTG format, that the remarks are entered.

C9.3.2.30 **Reverse Side, INT.** Indicate the initials (INT) of the person making the entry.

C9.3.2.31 **Reverse Side, Remarks.** Enter significant outage information necessary to document actions taken during fault isolation and restoration of service. The remarks must be detailed enough to reconstruct the events during later analysis.

C9.3.3 **DD Form 1697: Circuit Parameter Test Data - Analog.**
The purpose of DD Form 1697 is to record test and acceptance (T&A) data for initial acceptance of service and for recording periodic quality control test data on analog circuits. The CCO and CMOs and serving TCF and PTFs are required to maintain DD Form 1697s. A copy of the T&A report must be filed with the corresponding TSO in the circuit history files and be maintained for the life of the circuit. Periodic quality control (QC) test data must also be maintained in the circuit history files until the next annual QC is performed, at which time previous periodic QC forms may be discarded.

C9.3.3.1 **Block 1, CCSD.** The full command communications service designator (CCSD) for the circuit, as specified in the TSO.

C9.3.3.2 **Block 2, Type Test.** Type of test being performed on the circuit as specified in the QC schedule (e.g., T&A for test and acceptance, A for annual, SA for semiannual).

C9.3.3.3 **Block 3, Parameter Code.** Parameter code designated in the TSO for the circuit under test.

C9.3.3.4 **Block 4, Time Start (DTG).** Date and time in date time group (DTG) format (e.g., 010001Z JAN 12 that test began).

C9.3.3.5 **Block 5, Time Finish (DTG).** Date and time in date time group (DTG) format that test was completed.

C9.3.3.6 **Block 6, Receive Station/Initials.** Local facility designation and initials of operator performing the test at that facility.

C9.3.3.7 **Block 7, Transmit Station/Initials.** Distant facility designation and initials of operator performing the test at that facility.

C9.3.3.8 **Test.** Specific test to be performed from chapter 6.

C9.3.3.9 **Specifications.** Technical specifications of trunk or circuit in accordance with DISAC 300-175-9, Global Information Grid (GIG) Operating-Maintenance Electrical Performance Standards (reference 4.4).

C9.3.3.10 **Receive.** Readings recorded at the local facility. Initial reading taken and reading after adjustment was made, if necessary.

C9.3.3.11 **Transmit.** Readings recorded at the distant facilities receive (originating station transmit). Initial reading taken and reading after adjustment was made, if necessary.

C9.3.3.12 **Block 8, Test Tone Level.** Self-explanatory (1004 Hz, -10 dBm0).

C9.3.3.13 **Block 9, C-MSG Noise.** Noise reading taken strictly on critical control circuits (C3) or current transformer (CT) circuits that are analog end-to-end. If there are any pulse

code modulation (PCM) segments on the circuit, C-notched noise must be used. Refer to DISAC 300-175-9 (reference 4.4) for details.

C9.3.3.14 **Block 10, C-Notch Noise.** Noise reading taken on all analog and digital circuits, except those C3 and CT circuits that are analog end-to-end. Refer to DISAC 300-175-9 (reference 4.4) for details.

C9.3.3.15 **Block 11, Signal-to-Noise Ratio.** Signal to C-notched noise ratio. A ratio of the difference between actual signal level and C-notched noise level, measured in dB. Refer to DISAC 300-175-9 (reference 4.4) for details.

C9.3.3.16 **Block 12, Impulse Noise (IPN).** Measurement made to detect significant noise bursts. DISAC 300-175-9 (reference 4.4) specifies a maximum of 15 counts in 15 minutes above the reference level.

C9.3.3.17 **Block 13, Envelope Delay.** Readings taken to determine absolute delay caused by active components in transmission lines, measured in microseconds.

C9.3.3.17.1 **Spectrum.** Range of acceptable delay, in accordance with standards specified in accordance with DISAC 300-175-9 (reference 4.4).

C9.3.3.17.2 **Relative Delay.** Amount of delay allowed for a specific frequency range where each reading in that range is compared to a common, or relative, reading. Refer to Supplement 1 to DISAC 310-70-1, DII Technical Control Test Descriptions (reference 4.8) for detailed instructions.

C9.3.3.18 **Block 14, Frequency Response.** Amplitude versus frequency measured in dBs.

C9.3.3.18.1 **Spectrum.** Range of operating frequency response, as prescribed in DISAC 300-175-9 (reference 4.4) and Supplement 1 to DISAC 310-70-1 (reference 4.8).

C9.3.3.18.2 The + and - columns are tolerances allowed for each frequency range in accordance with DISAC 300-175-9 (reference 4.4). Allowances are relative to 1004 Hz.

C9.3.3.19 **Block 15, Net Loss Variation.** The variation in the receive level normally measured with a strip chart recorder in dBs over a 15-minute period.

C9.3.3.20 **Block 16, Change in Frequency.** The difference between the transmitted frequency and received frequency to nearest 0.1 Hz (recorded over 10 second period).

C9.3.3.21 **Block 17, Remarks.** Additional space for the tester to include any significant remarks concerning the tests. This is valuable for future analysis, especially if abnormalities were found.

C9.3.3.22 **Block 18, Signature of Tester.** Signature of individual who performed the test and recorded the test data.

C9.3.3.23 **Frequency Response (reverse side).** Individual frequency response readings taken during actual test in accordance with Supplement 1 to DISAC 310-70-1 (reference 4.8) must be recorded on the graph.

C9.3.3.23.1 **Receive.** Actual received levels are recorded in one column, then the relative (to 1004 Hz) is recorded in another column. For example, if the 1004 Hz reading was -10 dBm0 and the 500 Hz reading was -9.5 dBm0, the relative reading at 500 Hz would be -.5 dB. Relative readings for frequency response are noted as more loss and less loss; thus, a -9.5 dBm0 compared to a -10 dBm0 is .5 dB less loss, or -.5 dB.

C9.3.3.23.2 **Send.** Readings recorded at the distant facility are recorded in the same manner as receive readings.

C9.3.3.24 **Envelope Delay (reverse side).** Individual envelope delay readings taken during actual test, in accordance with Supplement 1 to DISAC 310-70-1 (reference 4.8) must be recorded on the graph.

C9.3.3.24.1 **Receive.** Readings recorded at the local facility receive the following attention: actual delay readings are recorded in one column and the relative delay is recorded in another column.

C9.3.3.24.2 **Send.** Readings recorded at the distant facility are recorded in the same manner as receive readings.

C9.3.3.25 **Frequency vs Amplitude.** Graph relative frequency versus amplitude response in dB.

C9.3.3.26 **Frequency vs Delay.** Graph relative frequency versus delay distortion in microseconds.

C9.3.4 DD Form 1697-1: Circuit Parameter Test Data - Digital. DD Form 1697-1 is used for the same purpose as the DD Form 1697 except it is to record results of digital trunks and circuits. Retention requirements are the same.

C9.3.4.1 Block 1, CCSD. The command communications service designator (CCSD) assigned to the circuit or trunk, as specified in the TSO.

C9.3.4.2 Block 2, Type Test. Type of test being performed on the circuit or trunk (e.g., T&A, annual, semiannually).

C9.3.4.3 Block 3, Time Start (DTG). Date and time in date time group (DTG) format (e.g., 010001Z JAN 12 that test began).

C9.3.4.4 Block 4, Time Finish (DTG). Date and time in date time group (DTG) format that test was completed.

C9.3.4.5 Block 5, Parameter Code. Parameter code designated in the TSO for the circuit or trunk under test.

C9.3.4.6 Block 6, Data Rate. Data rate used for testing the circuit or trunk (e.g., 9.6 Kbps, 64 Kbps).

C9.3.4.7 Block 7, Type Interface. Type of physical interface used on the circuit or trunk (e.g., RS-232, RS-449, V.35, MILSTD 188-114).

C9.3.4.8 Block 8, Type Sync. Type of synchronization utilized by the circuit under test (e.g., asynchronous, synchronous, isochronous).

C9.3.4.9 Block 9, Type Signal. Type of signal or coding utilized on the circuit or trunk being tested (e.g., non-return-to-zero (NRZ), bipolar, alternative mark inversion (AMI), B8ZS).

C9.3.4.10 Block 10, Test Pattern. Test pattern being used to test the circuit (e.g., 511, 2047, $1 \times 10^{20} - 1$).

C9.3.4.11 Block 11, Block Size. Block size being used to test the circuit (e.g., 100 bits, 1000 bits).

C9.3.4.12 Block 12, Receive Station/Initials. Local facility designation and initials of operator performing the test at that facility.

C9.3.4.13 **Block 13, Transmit Station/Initials.** Distant facility designation and initials of operator performing the test at that facility.

C9.3.4.14 **Test Column.** Specific test to be performed in accordance with chapter 6.

C9.3.4.15 **Specifications.** The required test time in minutes and standards for the circuit or trunk, as listed in DISAC 300-175-9 (reference 4.4).

C9.3.4.16 **Error Data.** Describes the type of error data to be recorded.

C9.3.4.17 **Receive.** Readings observed on the receive (local) end of the trunk.

C9.3.4.18 **Transmit.** Readings observed on the distant end receive of the trunk.

C9.3.4.19 **Block 14, Bit Error Rate.** Results of bit error rate test (BERT) as defined in Supplement 1 of DISAC 310-70-1 (reference 4.8).

C9.3.4.20 **Block 15, % Error Free Seconds.** Results of percentage (%) of error free seconds (%EFS) as defined in Supplement 1 of DISAC 310-70-1 (reference 4.8).

C9.3.4.21 **Block 16, % Block Error.** Results of percentage (%) of block errors as defined in Supplement 1 of DISAC 310-70-1 (reference 4.8).

C9.3.4.22 **Block 17, Telegraph Distortion.** Results of telegraph distortion test as defined in Supplement 1 of DISAC 310-70-1 (reference 4.8), typically a low speed (less than 150 baud) d.c. circuit.

C9.3.4.23 **Block 18, Remarks.** Indicate whether the circuit or trunk passed or failed the quality control (QC) tests as required by the specifications. Include any additional remarks regarding problems encountered during testing, remarks which may assist someone else in troubleshooting a specific problem, or any other comments which would aid another individual when testing this circuit or trunk.

C9.3.4.24 **Block 19, Signature of Tester.** Signature of the individual at the receive facility who completed and recorded the test data.

C9.3.5 **DD Form 1753: Master Station Log.** The Master Station Log (MSL) is the official narrative record maintained to record significant events (e.g., power failures, complete system outages, major equipment outages or impairments such as hazardous conditions (HAZCONs), and any other event that may have an impact on operation of the GIG, time verification, shift or watch changes, special tests, etc. Every GIG TCF and PTF and FCO must maintain a MSL. Other GIG facilities such as transmitter and receiver sites, microwave and radio relay sites, maintenance support activities, etc., must also maintain MSLs. When facilities are colocated, only one MSL is required as long as the MSL contains the narrative record for all colocated facilities. Reference may be made to supporting documents (outage tickets, equipment work orders, and status reports, as addressed in DISAC 310-55-1 (reference 4.1), etc.).

C9.3.5.1 Entries must be made in chronological order.

C9.3.5.2 The shift supervisor is normally required to sign "on" and "off" duty on the MSL.

C9.3.5.3 A hard copy of the MSL must be filed at the end of each RADAY.

C9.3.5.4 If the MSL is automated, the system must be password protected and require the shift supervisor to log "on" and "off" duty. It is also advisable to design the system so that it does not allow alterations.

C9.3.5.5 MSLs must be maintained for 11 months after the end of each month.

C9.3.5.6 Initials of the individual making the log entry.

C9.3.5.7 Narrative explanation of the action or event. Enter sufficient detailed information to fully explain the situation. Common abbreviations may be used.

C9.4 **Service Provisioning Records.** Each TCF and PTF must establish and maintain permanent history files for all links that terminate at their facility, all trunks and circuits that have physical patching capabilities within the TCF and PTF,

and all trunks and circuits for which the TCF and PTF is the CCO and CMO or servicing TCF and PTF. Circuit history files are not required for through facility trunks and circuits that do not have physical appearances, unless the TCF or PTF is the CCO and CMO or servicing TCF and PTF. Temporary circuit history files must be established on all trunks and circuits by each TCF and PTF addressed in the DISA TSO, regardless of patching capabilities. The temporary file must be maintained until the link, trunk, or circuit has been in-effected. Once in-effected, the temporary file may be discarded, unless a permanent history file is required by the above criteria. Colocated facilities (within the same building) are only required to maintain one history file. Each history file must contain a copy of the following:

C9.4.1 The initial test and acceptance data (DD Form 1697 or 1697-1).

C9.4.2 Copies of the latest TSO that reflects the current end-to-end configuration, control office assignment, etc.

C9.4.3 In-effect, exception, and delayed service reports applicable to the latest TSO. (When an exception or delayed service report is submitted that pertains to an intermediate facility, the intermediate facility must maintain their history file until the condition causing the report to be rendered is cleared and an in-effect report is submitted.)

C9.4.4 Status Acquisition Message (SAM).

C9.4.5 Copies of quality control waiver requests and approvals.

C9.4.6 Copies of any appropriate documentation (e.g., QC results, letters, etc.) resulting from action(s) taken to resolve degradations when a trunk or circuit fails management threshold for 2 consecutive months or more. (Documentation must be kept on file for 1 year.)

C9.5 Reference Library. A basic reference library must be maintained in each GIG TCF and FCO. Other manned GIG facilities responsible for performing technical control functions (e.g., PTF, radio relay sites, switching centers) are only required to maintain a limited library. Unmanned GIG facilities are not required to maintain a reference library.

Colocated facilities may maintain a common library if it is easily accessible to those personnel performing technical control functions. DISA Network Operations Centers (DNCs), using the guidelines established in this chapter, should develop publications requirements for each type of facility within their area of responsibility (e.g., TCF, PTF, DSN, DMS, AMHS, wideband facility, HF facility).

C9.5.1 DISA Numbered Publications. The following is a listing of publications relevant to the daily operations and management of a TCF, PTF, or FCO. At a minimum, the current editions of the DISA numbered publications marked with an asterisk are required in hard copy for a basic library. All other publications may be accessed by the Internet or maintained in soft copy form.

C9.5.1.1 *Supplement 1 to DISA Circular (DISAC) 310-70-1, DII Technical Control Test Descriptions.

C9.5.1.2 *DISAC 310-55-1, Status Reporting.

C9.5.1.3 DISAC 310-65-1, Circuit and Trunk File Data Elements and Codes Manual of the Global Information Grid (GIG).

C9.5.1.4 *DISAC 310-70-1, Global Information Grid (GIG) Technical Control.

C9.5.1.5 DISAC 310-D70-30, Global Information Grid (GIG) National Gateway Center (NGC) and Subscriber Operations (if applicable).

C9.5.1.6 DISAC 800-70-1, Operation and Control of the Defense Satellite Communications System (if applicable).

C9.5.1.7 DISAC 310-70-57, Defense Information System Network (DISN) Quality Assurance (QA) Program.

C9.5.1.8 DISAC 310-130-1, Submission of Telecommunications Service Requests.

C9.5.1.9 DISAC 310-130-2, Management Thresholds and Performance Objectives.

C9.5.1.10 *DISAC 310-130-4, Defense User's Guide to the Telecommunications Service Priority (TSP) System.

C9.5.1.11 DISA-DITCO Circular 350-135-1, Defense Commercial Communications Acquisition Procedures. (For GIG facilities having leased facilities or circuits. [This publication is available on the DISA DITCO Home Page at <http://www.ditco.disa.mil/corporatelibrary/home.asp>.])

C9.5.1.15 *DISAC 300-175-9, Global Information Grid (GIG) Operating-Maintenance Electrical Performance Standards.

C9.5.1.16 *DISAC 350-195-2, Auxiliary Electric Power Systems.

C9.5.1.17 *DISAC 310-55-9, Base Level Support for the Defense Information System Network (DISN).

C9.5.2 **Military Standards.** The following military standards (MIL-STDs) are available for distribution. Those GIG facilities required to maintain a basic reference library are encouraged to maintain the following MIL-STDs designated with an asterisk. These standards are available at <http://www.disa.mil/main/about/publications.html>. (MIL-STD-188/190, Methods for Communications Systems, 31 January 1990, and any subsequent revisions or change notices are inactive for new design and shall no longer be used for new designs.)

C9.5.2.5 MIL-STD-188-114A (13 DEC 1991//Change Notice 1), Electrical Characteristics of Digital Interface Circuits.

C9.5.2.6 MIL-STD-188-115 (17 DEC 1998//Change Notice 1), Interoperability and Performance Standards for Communications Timing and Synchronization Subsystems.

C9.5.2.7 MIL-STD-188-124B (18 DEC 2000//Change Notice 3), Grounding, Bonding and Shielding for Common Long Haul/Tactical Communications Systems Including Ground Based Communications-Electronics Facilities and Equipments.

C9.5.2.8 MIL-STD-188-140A (01 MAY 1990), Equipment Technical Design Standards for Common Long Haul/Tactical Radio Communications in the Low Frequency Band and Lower Frequency Bands.

C9.5.2.9 MIL-STD-188-145 (24 OCT 2000//Valid Notice 2), Interoperability and Performance Standards for Digital LOS Microwave Radio Equipment.

C9.5.2.10 *MIL-STD-188-154A (31 DEC 1997), Interface Subsystem, Equipment, and Interface Standards for Common Long Haul and Tactical Telecommunications Control Facilities.

C9.5.2.12 MIL-STD-188/190 (31 JAN 1990), Methods for Communications Systems Measurement.

C9.5.2.13 MIL-STD-188-200, System Design and Engineering Standards for Tactical Communications. (28 JUN 1983)
(Replaces MIL-STD 188-100 and MIL-STD-188C)

C9.5.3 **Military Handbooks.** The following military handbooks (MIL-HDBKs) are available for distribution. Those GIG facilities required to maintain a basic reference library are encouraged to maintain the following MIL-HDBKs designated with an asterisk.

C9.5.3.1 MIL-HDBK-232A (25 July 1988 and revalidated for acquisition 24 October 2000), RED/BLACK Engineering-Installation Guidelines.

C9.5.3.2 *MIL-HDBK-411B Vol. 1, 2 and 3 (15 May 1990)
(revalidated for acquisition -- 24 October 2000), Power and Environmental Control for the Physical Plant of DoD Long Haul Communications.

C9.5.3.3 MIL-HDBK-412 (20 May 1981) (revalidated for acquisition -- 24 October 2000), Site Survey and Facility Design Handbook for Satellite Earth Stations.

C9.5.3.4 MIL-HDBK-413 (28 March 1986 - Revalidated 24 October 2000), Design Handbook for High Frequency Radio Communications Systems.

C9.5.3.5 MIL-HDBK-415 (17 October 1994 -- Revalidated 24 October 2000), Design Handbook for Fiber Optic Communications Systems.

C9.5.3.6 *MIL-HDBK-419A (29 Dec 1987 Volumes 1 and 2), Grounding, Bonding and Shielding for Electronics Equipment and Facilities.

C9.5.3.7 MIL-HDBK-420 (20 March 1987 -- Revalidated 24 October 2000), Site Survey Handbook for Communications Facilities.

C9.5.4 **Allied Publications.** The current edition of Allied Communications Publication (ACP) 131, Communications Instructions Operating Signals, must be maintained in each GIG facility using teletypewriter orderwires or critical control circuits.

C9.5.5 **Technical Orders and Manuals.** Technical orders or manuals for each item of test equipment installed or used by personnel performing technical control functions must be available in the GIG facility. Technical orders or manuals for all terminal and ancillary equipment installed in the GIG facility must be available to personnel performing technical control functions.

Return to
Chapter 8
Basic Circular
Top of Table of Contents
DISA Publication Listing
DISA Home Page

Continue to:
Chapter 10

DISA PUBS@DISA.MIL - Last change: 21 March 2012

C10. CHAPTER 10. COMMERCIALLY LEASED CIRCUITS

C10.1 **General.** This chapter provides guidance for coordinating circuit actions for those circuits provided by commercial carriers, in accordance with policies outlined by the Defense Information Technology Contracting Organization (DITCO). DISA-DITCO CIRCULAR 350-135-1, Defense Commercial Communications Acquisition Procedures (reference 4.11), contains requirements for the submission of a DD Form 1368: Modified Use of Leased Communication Facilities, to DITCO, DISA headquarters (HQ), and the requestor. Technical Control Facility (TCF) or Patch and Test Facility (PTF) and Communication Control Office (CCO) or Communication Maintenance Office (CMO) management personnel should be thoroughly familiar with the provisions of DISA-DITCO 350-135-1 as it is the prescribing directive for leasing commercial circuits. DISA-DITCO 350-135-1 lists all guidance and policies regarding commercial leased circuits.

C10.2 **Categories.** For the purposes of Circular, leased circuits are divided into three categories: circuits provided by U.S. domestic carriers, circuits provided by U.S. international carriers (USICs), and circuits provided by foreign (non-U.S.) carriers.

C10.2.1 U.S. domestic leased communications services are usually procured from common carriers in accordance with the tariff provisions established with the Federal Communications Commission (FCC) and other regulatory bodies. Domestic carriers may not tariff the full range of parameters contained in the Global Information Grid (GIG) operating maintenance electrical performance standards. (Refer to DISAC 300-175-9, Global Information Grid (GIG) Operating-Maintenance Electrical Performance Objectives (reference 4.4), for domestic leased communications services.) Only those parameters that are tariffed are guaranteed. For services within the continental United States (CONUS), DITCO converts parameter codes contained in the Telecommunications Service Order (TSO) to the tariff offering of the carrier which will meet or exceed the parameters of the applicable GIG technical schedule.

C10.2.2 U.S. international carriers (USICs) generally bid to provide service, and contracts for the service are based on the parameters contained in the TSO. The USIC awarded the contract is then responsible for installing and maintaining the leased service within the cited parameters. The USIC may designate a representative to receive and act upon telecommunications

requests (TRs) in those areas where the carrier does not have an office. The DITCO status acquisition message (SAM) will provide telephone numbers of commercial activity locations that will accept collect calls for trouble reporting purposes at both end terminals. (Refer to DISA-DITCO 350-135-1 (reference 4.7) for information regarding SAM messages.)

C10.2.3 Foreign carriers are frequently owned by the government of the country in which they operate. DITCO procures the portion of international leased services provided by foreign carrier through the USIC, whenever possible. Their methods of operation are prescribed by the foreign government, and the service offered under the rates, rules, and regulations of the foreign carrier administrations may or may not conform to International Telecommunication Union - Telecommunication (ITU-T) standardization recommendations. In many areas, foreign carriers do not provide for working overtime, during weekends, or during national holidays. However, the USICs have a 24-hour central trouble call desk.

C10.3 Meeting and Maintaining Technical Sufficiency.

C10.3.1 Circuits within CONUS are normally leased from one carrier under a "single Communications Service Authorization (CSA)" concept. This means that, to the extent possible, DITCO selects a single carrier to provide for the overall service and to make arrangements, as necessary, with other carriers participating in providing the service to furnish modems, conditioning, transmission paths, etc., as appropriate. Terminal equipment may either be leased under the same CSA or separately, or may be government furnished. The carrier performs all coordination necessary to establish and maintain the quality of service ordered between terminals shown in the CSA and for providing required signals and signal levels (as specified in the CSA) where government and leased facilities interface. The carrier does not perform end-to-end service when the circuit specified in the CSA is a segmented lease and is extended past the end terminals shown (i.e., by GIG multiplex or channel packing systems, by military facilities, etc.).

C10.3.2 Circuits leased between CONUS and Alaska and circuits leased between CONUS and Canada are normally procured on a segmented basis from different carriers. The carriers perform only for the portion of the service specified in their contracts. In the event a carrier providing service fails to respond to TCF and PTF requests to isolate and correct circuit

problems, the Systems Control Officer (SCO) of the servicing DISA Network Ops Center (DNC) should be contacted immediately for assistance.

C10.3.3 For leased services provided entirely by common carrier facilities, the USIC must provide technical sufficiency end-to-end, including connecting facilities provided by arrangement with the U.S. domestic and with foreign carriers.

C10.3.3.1 For transoceanic services, the composition of which is predominantly common carrier, as determined by the government, but which contains government-owned segments, the carrier awarded the contract must provide the technical sufficiency of the service end-to-end, including connecting facilities provided by arrangement with U.S. domestic, USICs, and with foreign carriers.

C10.3.3.1.1 The carrier awarded the contract will engineer the service on an end-to-end basis and will provide the government with the technical parameters necessary to condition the government-owned segment to meet the overall transmission requirement. The government will provide, install, and maintain the equipment necessary to condition and terminate government owned segments.

C10.3.3.1.2 The government and the carrier will establish a demarcation point for determining outages chargeable to the carrier for all transoceanic circuits. The demarcation point will be the location where the government-owned segment meets the common carrier segment. However, where the demarcation point does not clearly separate government and commercial equipment or facilities, the ownership of the equipment or facilities will determine maintenance responsibility.

C10.3.3.1.3 The USIC awarded the contract will perform all testing and other actions necessary to maintain the continuity and quality of service end-to-end without regard to the demarcation point established between government-owned segments and common carrier segments.

C10.3.3.2 For transoceanic service, the composition of which is predominantly government owned, as determined by the government, but which contains a common carrier segment, the government is accountable for the technical sufficiency end-to-end.

C10.3.3.2.1 The government will engineer the service end-to-end and will order from the commercial carrier the tariffed offering which meets or exceeds the parameters required to meet the overall transmission requirements when the segments are connected in tandem. The carrier awarded the contract will provide, install, and maintain the equipment necessary to condition and terminate the carrier-owned segment, except when the government specifies that government-furnished equipment will be used.

C10.3.3.2.2 The government and the carrier will establish a demarcation point for determining outages chargeable to the carrier. The demarcation point will be designated in the TSO submitted to DITCO and will be made a matter of record in the order or contract covering the service. The demarcation point will be the location where the government-owned segment meets the common carrier segment. However, when the demarcation point does not clearly separate government and commercial equipment or facilities, ownership of the equipment or facilities will determine maintenance responsibility.

C10.3.3.2.3 The government will control all testing and other actions necessary to maintain the continuity and quality of service end-to-end without regard to the demarcation point established. The government will accomplish the testing of common carrier segments in coordination with the control office designated by the international carriers.

C10.3.4 The TSO will designate a facility or DISA implementations office which will accept leased service on behalf of the government.

C10.3.4.1 Initial test and acceptance (T&A) data will be used as the baseline for those circuits unable to meet all parameters specified in the appropriate technical schedule. Whenever a major realignment of facilities which the circuit traverses is accomplished, or when measured performance of facilities is obtained as a result of a technical evaluation program visit, the new data obtained for circuit performance will be used as the baseline.

C10.3.4.2 Circuits failing to meet all parameters specified in the appropriate technical schedule when T&A is performed will not be accepted for service by the Communication Control Office (CCO) or Communication Maintenance Office (CMO) without approval of the TSO issuing authority.

C10.4 Initial Acceptance of Leased Service. The TSO will designate a GIG facility or DISA implementation office which will accept leased service on behalf of the U.S. Government. If the leased service traverses at least one GIG TCF or PTF, then the TCF or PTF will be assigned as the Communications Control Office (CCO) responsible for accepting service. When service is in support of a GIG backbone or DISA initiated order, as requested by the customer of the requirement, the TSO will designate a DISA authority for government acceptance. Otherwise, the TSO must designate a Communications Management Office (CMO) to accept service. The CCO or CMO will ensure leased circuit segments meet all circuit parameters for the type of service specified in the SAM and contact the TSO issuing authority when the carrier fails to meet all required circuit parameters. The TSO issuing authority will determine whether service will be accepted or will obtain such a determination from the requestor or telecommunications request (TR) issuing authority. The CCO or CMO submits required completion reports as follows:

C10.4.1 If the circuit meets all required parameters, as specified in DISA-DITCOC 350-135-1 (reference 4.11), and the user has satisfactory service, an in-effect report (IER) will be submitted. The circuit will be maintained within these parameters.

C10.4.2 If the circuit does not meet all required parameters and the TSO issuing authority advises that the circuit must meet these parameters prior to accepting the service, a delayed service report (DSR) will be submitted advising that the carrier is unable to provide required service on the date specified in the TSO.

C10.4.3 If the circuit does not meet all required parameters and the TSO issuing authority advises that the circuit may be accepted for service, an exception report will be submitted. Until the exception report is cleared (e.g., the carrier corrects all circuit deficiencies or the requestor authorizes a change in parameters or other technical aspects), measured test data during the initial T&A will be maintained as temporary baseline data until the responsible carrier corrects all circuit deficiencies. The TSO issuing authority is accountable for necessary action to ensure the exception report is subsequently cleared. Once all exceptions are cleared, an IER will be submitted.

C10.5 **Circuit Problems.** Upon activation of a circuit, users are to report any degradations or outages to the serving TCF and PTF for corrective action.

C10.5.1 When a leased service is interrupted or fails to meet the parameters prescribed in the DITCO Status Action Message (SAM) (for reasons other than customer negligence or failure of facilities furnished by the customer), the serving TCF or PTF will immediately log the circuit out of service with the responsible carrier. If there is no serving TCF or PTF, the user is accountable for reporting the degradation or outage directly to the carrier and for informing the CCO or CMO of the situation. If satisfactory action is not taken by the carrier on problems that affect service, the situation should be documented on a DD Form 1368: Modified Use of Leased Communication Facilities, and forwarded in accordance with DISA-DITCO 350-135-1 (reference 4.11). In cases where the circuit has a history of substandard performance, DITCO may elect to change carriers based on submission of the DD Form 1368 and in accordance with the procedures of the leasing activity.

C10.5.2 Prior to reporting an outage to the commercial carrier, the TCF or PTF will attempt to isolate the trouble if any government-furnished terminal equipment or circuit segment is used. When the trouble is isolated to the government-furnished segment or equipment, including equipment leased under Federal Supply Schedules, the failure will not be reported to the common carriers. The government is subject to a maintenance-of-service charge when trouble reported to the carrier is subsequently isolated to equipment or facilities provided by the government.

C10.5.3 Whenever an outage attributable to a leased segment occurs, regardless of the direction of outage (send or receive), the carrier providing end-to-end technical sufficiency or an authorized representative will be notified of the outage. The serving TCF or PTF or user when there is no TCF or PTF will notify the appropriate carrier representative of the outage to preclude unnecessary delay in circuit restoration. The time the carrier or authorized representative is first notified of the outage by the TCF or PTF or the user is the time that the commercial segment is considered to be out of service. Leased circuits logged out of service are considered to be out in both directions and reroute actions must include send and receive paths.

C10.5.4 When the carrier returns the circuit to service, the TCF or PTF will perform those quality control (QC) tests which are necessary to establish that the circuit meets required parameters. When the user establishes end-to-end contact on the circuit and is satisfied with the performance, the TCF or PTF will log the circuit back to service.

C10.5.5 Care must be exercised when turning a circuit over to the carrier to "check" circuit operation. Unless the carrier is specifically advised that the circuit is "logged out" of service, the carrier may decline to accept circuit outage even though the cause for degraded service is subsequently identified as a carrier problem. Outage time chargeable to the carrier begins at the time the TCF or PTF or user notifies the carrier that the circuit is out of service. Chargeable outage time is considered terminated when the carrier notifies the TCF or PTF or the user that the problem has been corrected, unless the carrier is notified within 30 minutes that the problem still exists.

C10.6 TCF and PTF Cooperation With Commercial Carriers.

C10.6.1 TCF and PTFs are required to cooperate with the carriers to activate circuits and to restore disrupted service as soon as possible. However, it is not the responsibility of the TCF or PTF to perform unlimited test measurements for the carrier after a circuit has been logged out of service. Once the TCF or PTF has determined that a circuit is out of service due to leased facilities, it becomes the carrier's responsibility to isolate and correct all circuit problems.

C10.6.2 The TCF or PTF will provide the carrier with test measurement data obtained when carrier facilities are determined to be the cause of the outage. The data may assist the carrier in isolating the trouble but does not necessarily indicate that other parameters are within required specifications. When the carrier returns the circuit to the TCF or PTF, the carrier is, in effect, stating that the circuit meets all of the circuit parameters contained in the SAM. If subsequent tests performed by the TCF or PTF show that the carrier has not fully restored the service, the TCF or PTF may request the carrier to perform test measurements on the leased segment(s) of the circuit from the point of interface between the government and the carrier. Difficulties in obtaining the cooperation of the carrier must be fully documented and immediately reported to appropriate requestor for further action.

C10.6.3 Since GIG procedures and standards cannot be imposed on commercial entities, an understanding of commercial procedures and standards is frequently necessary when dealing with U.S. and foreign carrier personnel. TCF or PTF supervisory personnel should arrange to meet with representatives of commercial carriers providing leased services to their facilities.

C10.7 Scheduled Outages.

C10.7.1 The DISA Network Ops Center (DNC) coordinates the scheduling of planned commercial facility outages which will affect GIG leased circuits; therefore, outages must be coordinated with individual users.

C10.7.1.1 The carriers occasionally require that certain multichannel facilities be removed from service to perform necessary repairs, cutovers, power improvements, quality control (CQ) testing, etc. The carrier must reroute or otherwise provide service to GIG users during facility outages, and the outages should be scheduled for the nonbusy period of the users. When the carrier cannot reroute the individual services on an uninterrupted basis during a planned facility outage, the carrier must notify the DNC of the nature and estimated duration of the outage. The DNC element approving the outage will ensure the affected TCF or PTFs and control offices are advised of the approved outage.

C10.7.1.2 A circuit release is granted for the time requested by a carrier to perform periodic routine maintenance, implement required circuit changes, or accomplish other actions that require removing a circuit from service on a previously scheduled basis. Circuit releases are granted for a specified time which is mutually agreeable by the user and the carrier. Circuit releases are not granted to correct deficiencies on circuits previously logged out of service by the TCF and PTF or for those circuits being used on an impaired basis.

C10.7.1.2.1 United States Immediate Carriers (USICs) will direct all requests for GIG circuit release to the appropriate DNC. The DNC will effect necessary coordination with subordinate DNC elements, the TCF or PTFs, and users to obtain the circuit release and will confirm the approval of the request with the carrier or schedule an alternate release time.

C10.7.1.2.2 Domestic carriers will direct all requests for GIG circuit releases to the DNC. The DNC will initiate necessary coordination with the TCF or PTFs and users in DISA areas 1, 2, 6, and 9 to obtain the circuit release. The decision rendered by the DNC will be disseminated by telephone to the facilities, users, and agencies involved.

C10.7.1.2.3 Foreign carriers will direct all requests for circuit release to the appropriate servicing TCF or PTF. The servicing TCF or PTFs will obtain user concurrence and advise other TCFs or PTFs in the circuit and appropriate DNC elements of the scheduled outage prior to notifying the foreign carrier that the release time is acceptable.

C10.7.1.3 When a carrier is unable to complete necessary actions within the time period authorized, requests for extension for the planned facility outage or circuit release will be processed as outlined above.

C10.7.2 Commercial carrier outages, scheduled or unscheduled, must be reported on DD Form 1368: Modified Use of Leased Communication Facilities, by the facility designated in the TSO for reimbursement of service not provided.

C10.8 Impaired Service.

C10.8.1 Occasionally, it is necessary to accept service from a commercial carrier on an impaired service basis when quality control (QC) tests indicate one or more technical schedule parameters are out of tolerance and the carrier is not in a position to fully restore the service. The following guidelines apply:

C10.8.1.1 The TCF or PTFs may accept circuits for service on an impaired basis when the user is able to pass required traffic on the circuit and agrees to accept the service on an impaired basis, and the carrier estimates that normal service can be provided within 3 days.

C10.8.1.2 When corrective action has not been accomplished by the carrier within 3 calendar days of the date service was accepted on an impaired basis, the TCF or PTF will initiate action with the appropriate DNC element to escalate the problem to higher levels for assistance in expediting restoration of service to normal.

C10.8.1.3 Appropriate DNC elements will be notified whenever a circuit is placed in an impaired service status. Notification will include identification of the carrier, nature of the impairment, and date the circuit is scheduled to be fully restored to service. Appropriate DNC elements will also be notified when service has been fully restored.

C10.8.1.4 Circuits accepted for service on an impaired basis are not considered out of service for DISAC 310-55-1, Status Reporting (reference 4.1), or DD Form 1368 reporting purposes.

C10.8.1.5 Circuits that fail to pass required traffic will be logged out of service, and the carrier will be required to restore service as soon as possible.

C10.8.1.6 Excessive occurrences of a circuit being placed in an impaired service status will be documented and reported to the TSO issuing authority for corrective action.

C10.8.2 Accepting circuits for service on an impaired basis is a judgment decision made by the CCO acting as the agent of the government. DNC elements will assist the CCO in making this decision, if required.

C10.8.3 The government is liable for the payment of the full recurring charges for the service during all periods of acceptance on an impaired basis.

C10.9 Quality Control (QC) Testing. The requirement for QC testing of leased circuits is identical with that required on government-owned circuits. (Refer to chapter 6 for specific test requirements.) The Communications Control Office (CCO) will coordinate QC test schedules with commercial carriers to ensure the carriers will have personnel and test equipment available to conduct QC tests. The CCO will notify the appropriate requestor of any commercial carriers refusing to participate in scheduled out-of-service QC testing. The requestor should then verify the terms of the lease and either contact the carrier to arrange scheduling or initiate a request for QC testing. When the TCF or PTF is relieved of the responsibility for conducting QC tests on specific circuits, all outages attributed to the carrier on those circuits will be reported to the carrier as "not providing required service."

C10.9.1 Leased international and transoceanic circuits for channel-packed trunks extend from servicing TCF or PTF to serviceing TCF or PTF. The commercial lease and the channel-pack lease are separate contracts and are tested and reported separately. The commercial carrier awarded the contract is accountable for the technical sufficiency of the circuit between serving TCF or PTFs. Leased circuits between serving TCF or PTFs and users are ordered by separate DITCO action. The domestic or foreign carriers providing tail segments are accountable for the technical sufficiency of the tail segments they provide. (Refer to chapter 6 for segmented testing requirements.)

C10.9.2 Provisions for QC testing by the USIC are outlined in individual CSAs which are issued by DITCO to the commercial agency providing the service. The CSA constitutes a written agreement between the government and the commercial carrier to conduct fault isolation, restoration, and QC testing on Defense Switched Network (DSN) Interswitch Trunks (ISTs). Scheduled periodic QC testing of DSN ISTs connecting an overseas military switching center with a commercial switching center in CONUS is not required. The TCF or PTFs responsibility for participating in initial QC and fault isolation testing is outlined in chapter 6. Additional QC requirements for CONUS and overseas ISTs are prescribed as follows:

C10.9.2.1 Testing will be scheduled in accordance with requirements identified in chapter 6, which is normally with the servicing military technical control in the overseas area. The CCO or CMO will forward the schedule to the appropriate DISA area 90 days prior to the start of the schedule.

C10.9.2.2 The DISA area will review the CCO or CMO schedules, resolve possible conflicts, and incorporate all inputs into an area QC schedule to be forwarded to HQ DISA, Code Disbursing Office Voucher (DOV), 60 days prior to the start of the schedule. Schedules will include, as a minimum, the command communications service designator (CCSD), commercial communications service authorization (CSA) number, circuit parameter from or to geographical location (GEOLOC), and scheduled test time. HQ DISA or DOV will review the area QC schedules, arrange coordination with the CONUS commercial agencies, resolve any conflicts, and notify the area QA division of required changes, or approval, no later than 30 days prior to start of the quarter.

C10.9.2.3 Deviation from the approved schedule must be coordinated with DOV, responsible DNCs, USIC, CONUS switching centers, and participating GIG TCF or PTFs. CCOs or CMOs must initiate advance coordination of scheduled tests to ensure availability of personnel and equipment necessary to meet testing requirements contained in chapter 6. Test schedule changes will be coordinated well in advance of scheduled time to minimize impact on personnel and equipment and to prevent the government from incurring additional charges from the vendor. All scheduled QC testing will be accomplished end-to-end under the purview of the CCO or CMO that will order testing with the CONUS switching centers on behalf of the government and will maintain strict accounting of the start and end times of testing to facilitate billing verification. The CCO or CMO will not, under any circumstances, order testing on behalf of USIC during fault isolation or correction.

C10.9.2.4 Intentional disruptions to DSN ISTs for any length of time are not authorized unless QC tests are to be conducted on the circuit in accordance with the DISA schedule and isolation and correction of a circuit problem is required.

C10.9.2.5 The commercial carrier is allocated 3 hours to perform QC tests on each IST.

C10.9.2.6 If a leased DSN IST fails to meet specifications during a scheduled QC test and the circuit cannot be realigned to specifications during the allocated 3 hours, the CCO has two options:

C10.9.2.6.1 Normally, the CCO or CMO will log the circuit out to the USIC and the circuit will remain out of service until all specifications are met.

C10.9.2.6.2 When operational circumstances dictate, the CCO or CMO may return the circuit to service in an "impaired" status if the circuit is capable of providing service for which it was leased. Prior to returning the circuit to service, the TCF or PTF will coordinate with the USIC and establish a firm date and time (within 3 days) when the impairment will be corrected.

C10.9.2.7 Only one IST between two switches should be removed from service for QC testing at a given time. The first circuit will be logged out and returned to service before the next IST is removed for testing.

C10.9.2.8 Test results will be recorded on DD Form 1697: Circuit Parameter Test Data - Analog, and maintained in the appropriate circuit history folders.

C10.10 Outage Reporting.

C10.10.1 GIG TCF or PTFs, CCO or CMOs, users, or other agencies designated in the TSO must, in accordance with DISA-DITCO 350-135-1 (reference 4.7), submit a report each month on those leased circuits experiencing outage attributed to the carrier. Outages caused by the failure of government-provided equipment or facilities, or due to negligence of government personnel, will not be included in this report.

C10.10.2 A DD Form 1368: Modified Use of Leased Communication Facilities, may also be submitted for services that suffer extended or frequent interruptions or when DITCO assistance is desired in seeking to improve the reliability of the leased service.

Return to:

Chapter 9

Top of Table of Contents

Basic Circular

DISA Publication Listing

DISA Home Page

DISA PUBS@DISA.MIL - Last change: 21 March 2012
