DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

APR 0 4 2014

DISA CIRCULAR 310-65-1*

CHANNEL AND CIRCUIT ALLOCATION

Circuit and Trunk Table Management for the Department of Defense Information Network

1. **Purpose**. This Circular describes the circuit and trunk table management for Department of Defense Information Network (DODIN). It identifies data codes authorized for use in the preparation and submission of Telecommunications Service Requests (TSRs) and Telecommunications Service Orders (TSOs).

2. **Applicability**. This Circular applies to all Department of Defense (DoD) and non-DoD departments, agencies, commands, and offices having authorized requirements for DODIN services or for other services that are acquired by DISA.

3. **Authority**. This Circular is published in accordance with the authority contained in DoD Instruction 8100.04, DOD Unified Capabilities (UC), 9 December 2010, and DoD Directive 5105.19, Defense Information Systems Agency (DISA), 25 July 2006.

4. **General**. This Circular is designed to assist in defining specific data elements listed in the software outputs from the circuit and trunk files that are managed as a table within DISA tools. All table data elements are created and managed by DISA to be incorporated into the DISA provided toolsets used as part of the Request Fulfillment and Release and Deploy (provisioning) processes. The specific element codes are maintained within DISA-provided databases, while change management of inclusive data are led by the Request Fulfillment Process Managers' designated offices and changes and/or updates issued as e-mail notifications when changes are made. The Defense Information Systems Network (DISN) Program Management Office (PMO) will act as governance and primary point of contact for final mitigation authority for any nonconformity.

5. **Organization of Chapters**. Each chapter contains the following paragraphs (at a minimum): general, definitions of terms, and use. As these paragraph headings appear in all of the chapters, the paragraph headings are not entered under the chapter titles in the table of contents.

6. **Office of Primary Responsibility for Files.** The Office of Primary Responsibility (OPR) for management control and operational direction required to maintain the files is Headquarters, DISA, Network Services Directorate (NS), unless specified otherwise in the chapters.

7. **Changes.** All recommendations for changes (content or format) are to be submitted to the DISN Program Management Office (PMO) for consideration. The DISN PMO will initiate internal change management process actions inclusion to the Agency meta-data database in the DoD metadata registry in the Data Services Environment at https://metadata.ces.mil. The DISN PMO has overall responsibility although the actual method and procedure may be delegated to the process manager layer for implementation. This guidance on changes applies to each element identified, unless specified otherwise.

FREDERICK A. HENRY
Brigadier General, USA
Chief of Staff

SUMMARY OF SIGNIFICANT CHANGES. This revision updates and further defines data table management within DISA provided tools. Many chapters have been removed and have been marked "Reserved," as they will be used for future use with other tables of record for above mentioned tools. The removal of these chapters designate technology changes, internal DISA use, system characteristics, etc., and are only identified within the table of contents and are not currently within the Circular; however, as the need arises, the table of contents and the Circular will be updated to include new information. Deleted information will be retained by the Defense Information Systems Network (DISN) Program Management Office (PMO) as the Office of Primary Responsibility (OPR) for possible future use or technology reference. The DISN PMO will act as governance, primary point of contact, and DoD meta-data collaboration on behalf of the telecommunications community.

---

*This Circular cancels DISAC 310-65-1, 23 January 2003 and must be reissued, canceled, or certified current within 5 years of its publication. If not, it will expire 10 years from its publication date and be removed from the DISA issuance postings.
OPR: NS - disa.meade.ns.mbx.disa-ft-meade-ns-mailbox
DISTRIBUTION: P

CONTENTS

ILLUSTRATIONS

Figure

C1. CHAPTER 1. OVERVIEW

C1.1 **General.** The Department of Defense Information Network (DoDIN) circuit and trunk files are computerized compilation of existing and planned utilization of DoDIN communications resources. Each file is designed to provide specific engineering, operational, and management data containing capabilities of National Communication System (NCS) and DoDIN resources. Circuit and trunk records are generated from Telecommunications Service Orders (TSOs). TSOs are generated by a Telecommunications Service Requests (TSRs). DISA-provided tools are migrating toward more automated set of data elements, which will be managed as "drop down" data codes and naming conventions that have been standardized for use across the enterprise, i.e., same data used to compile the TSR within correct tool will be used throughout order management process and entered as part of configuration management process and tools. This method will ensure data integrity and report creation requirements from the Defense Information Systems Network (DISN) Operations Support System (OSS) portal(s).

C1.2 **Definition of Terms.** Not applicable (N/A)

C1.3 **Use.**

C1.3.1 The previous Circuit and Trunk circular identified many information fields which are used jointly or individually to assist in the following activities: allocation of circuits and trunks, status reporting, planning and engineering of circuits and trunks, statistical analysis of resources, simulation studies, daily operation of operation centers, certification of restoration priorities, inventory of resources to operating agencies, and capacity planning and management or the consolidation or elimination of facilities or stations.

C1.3.2 Each of the above have diverse requirements for software-generated reports. The requirements may differ in format, content, and primary and secondary sort sequence, etc. Therefore, in addition to the standard circuit and trunk listings, output reports may be obtained by selecting any one or more data elements contained in the files in the format which the user desires.

C2. CHAPTER 2. TYPE OF SERVICE

C2.1 **General.** The type of service identifies the specific service to which the customer is requesting a telecommunication circuit. The types of services provided by DISA are described in the DISA Service Catalog.

C2.2 **Definition of Terms.** Character used is pre-set to delineate specific type of service ordered by customer. This character is the 4th character within 8-character command communications service designator (CCSD) (See chapter 14).

C2.3 **Use.** By indicating the correct type, the tools will then filter the required items needed to build the circuit requirement.

C3. CHAPTER 3. AGENCY REQUIRING SERVICE

C3.1 **General**. The Agency requiring service identifies the Government agency requiring the service. As used in this context, the term "agency" refers to the Government agency; e.g., Army, Navy, DISA, Air Force, Marines, DoD, etc., that requires the circuit being ordered in support of its mission. It is not intended to identify operations and maintenance (O&M) and funding agencies, although in many instances they are the same.

C3.2 **Definition of Terms.** Two letter character used is pre-set to delineate specific Agency requiring the service.

C3.3 **Use.** Many reports generated are for specific Service or Agency to which this field is used as one of the filters to narrow scope of mass data download.

C4. CHAPTER 4. AVOIDANCE

C4.1 **General.** Four data fields comprise the area of avoidance: location, network, transmission media, and other circuits. These data fields allow customers to request that a specific location, network, and transmission media to be avoided when engineering a solution of their requirement. The data inserted within these fields will be governed by tool management capability, and a drop down box will be enabled for customers to choose an option that is within the DISN.

C4.2 **Definition of Terms.**

C4.2.1 Location. Specific geographical locations or sites to be avoided;

C4.2.2 Network. Specific networks; and/or

C4.2.3 Transmission Media. Specific transmission medians to be avoided; and/or

C4.2.4 Circuits. Other circuits that currently exist, or have active Telecommunications Service Requests (TSRs) in the planning cycle, to be avoided.

C4.3 **Use.** Standardization of data elements allows for quicker filtering of required data when certification offices are engineering their networks for redundancy.

C5. CHAPTER 5. AGENCY CODE

C5.1 **General**. The Agency code is the first letter in the 8-character command communications service designator (CCSD) identifying the agency retaining "ownership." As used in this context, the term "agency" refers to the Government agency; e.g., Army, Navy, DISA, Air Force, Marines, DoD, etc. (See chapter 14 for full definition and use of the CCSD.)

C5.2 **Definition of Terms.** Single letter character used to delineate specific Agency owning the service being provided.

C5.3 **Use.** Many reports generated are for specific Service or Agency to which this field is used as one of the filters to narrow scope of mass data download.

C6. CHAPTER 6. DISA CONTROL NUMBER

C6.1 **General.** A DISA control number (DCN) is used for tracking and maintaining visibility of projects. When a customer funded project is entered into the project process, the DISA activity will assign a DCN commensurate with the customer's agency. The code is a four character alpha numeric with first character being the Agency code to which the customer belongs, the second character (a number) depicts the year in which the code was initiated, the third and fourth numerical code is sequential for that customer coding.

C6.2 **Definition of Terms.** Not Applicable

C6.3 **Use.** This element gives management visibility to all circuit actions that are required for a specific project. As such, metrics can be written to quickly account for overall status and milestones associated. The life cycle of the DCN is dependent upon the life cycle of the project and should not be used in subsequent changes that are unrelated to the project.

C7. CHAPTER 7. VIRTUAL PRIVATE NETWORK NAMING CONVENTION

C7.1 **General.** The DISN Private Internet Protocol (IP) service is an enterprise Virtual Private Network (VPN) service providing data privacy to mission partners across the SBU IP Data network (formerly known as NIPRNet). Features of this service include the following:

C7.1.1 DISA managed VPN using Multi-Protocol Labeled Switching (MPLS).

C7.1.2 Provides privacy and limits access to IP data to VPN members only.

C7.1.3 Connections available at Unclassified-Aggregation Router (U-AR) or Unclassified-Provider Edge router (U-PE).

C7.1.4 Quality of Service (QOS): provides the ability to provide different priorities to different pre-marked packets (applications, users, or data flows) or to guarantee a certain level of performance to those packets across the DISN. It does not provide on customer's traffic a higher priority than another customer's traffic.

To order this service the naming convention requires standardization. Private IP identifiers or IDs will be generated during the "Establish Private IP ID" process. Each Private IP will have a unique ID consisting of a Private IP name and number. Using a standard approach to the creation of the name allows the customer to generate automatically by the order entry tool, without unnecessary manual intervention, thus, streamlining the process and creating faster delivery of the "Establish Private IP ID" requirement. The full accounting is included as this is a newly developed service and not all tools have been adequately coded.

C7.2 **Definition of Terms.**

C7.2.1 The first part of the Private IP ID is the Private IP name. It consists of four alphanumeric characters:

Positions 1 – 2: Agency requiring the VPN service. Otherwise known as "TCO Code" as defined within DISAC 310-130-1, Submission of Telecommunications Requests.

Position 3 - 4: Type of VPN (new code):

1) Type of data. coded
2) Structure. alphanumeric
3) Length. 2 characters
4) Limitations. no blanks

L3	Layer 3 VPN (Private IP Service)
L2	Layer 2 VPN (Ethernet Private LAN Svc)
CX	CsC (MPLS Labeled Transport)
TE	Test and Evaluation Network (DTEN)
	(more codes may be added in the future)

C7.2.2 The second part of the Private IP ID is the Virtual Private Network (VPN) number, which consists of five numeric characters. This is a globally unique, five-digit, number. These numbers are assigned sequentially, from blocks of numbers identified by the Network Services Directorate (NS), and reserved for the various types of VPNs. The table below identifies the assigned number blocks.

VPN Number Assignments	
VPN Number	**VPN Layer**
00000 - 00200	Unassigned
00201 - 39999	AR/U-PE
40000 - 41999	DTEN/LES
42000 - 69999	Unassigned
70000 - 89999	IPT Layer
90000 - 99999	C-PE

a. The "L3" type VPN will receive assignments from the 00201 – 39999 block.
b. The "L2" type VPN will receive assignments from the 70000 – 89999 block.
c. The "CX" type VPN will receive assignments from the 70000 – 89999 block.
d. The "TE" type VPN will receive assignments from the 40000 – 41999 block

C7.3 **Use.** N/A

C8. CHAPTER 8. COMMUNICATION CONTROL OFFICE IDENTIFICATION - ACCEPTING AUTHORITY

C8.1 **General.** The Communication Control Office (CCO) or Circuit Management Office (CMO) is the designated authority for the circuit named within the requirement. This office monitors service performance accepting service on behalf of the U.S. Government. Their duties are detailed in DISAC 310-130-1, Submission of Telecommunications Requests, and DISAC 310-70-1, Global Information Grid (GIG) Technical Control. If there is not a designated office named within the Telecommunications Service Request (TSR), then DISA will insert the most logical office to which all responsibilities are to be assigned.

C8.2 **Definition of Terms.** In most DISA provided common user IP networks, DISA retains management authority and are listed within the Telecommunication Service Order (TSO) as the CMO.

C8.3 **Use.** Data element to be used as filter for office of responsibility for such actions as completion reports.

C9. CHAPTER 9. MODULATION RATE

C9.1 **General.** The modulation rate is in the drop-down option available for the rate at which the circuit will operate. If the circuit operates alternately at more than one modulation rate the highest modulation rate is used in conjunction with the fourth character of the command communications service designator (CCSD) to represent the transmission rate for the type of service specified. If the circuit operates at different data rates dependant on direction, customer is asked to enter the applicable data rate in the direction 1 and 2 fields.

C9.2 **Definition of Terms.** Bandwidth or modulation rate is a numerical representation of the portion of a given transmission path and/or link in which the customer's requirement will use for transmission.

C9.3 **Use.** Modulation or bandwidth is used in capacity planning for the Defense Information Systems Network (DISN) build-out, DISN Subscription Service, and Certification Offices as a cross-check on allocation of assets for mission completion.

C10. CHAPTER 10. CIRCUIT PARAMETERS

C10.1 **General.** The circuit parameters represent the technical characteristics of the circuit and to the level of testing parameters to be used during quality control checks. The technical schedules (parameters) specific to services are described within DISAC 300-175-9, Global Information Grid (GIG) Operating-Maintenance Electrical Performance Standards. Technical standards for leased circuits should be clearly identified (in full text) in the award documentation (Contract Performance Work Statement) provided to the vendor.

C10.2 **Definition of Terms.** The circuit parameter represents the technical characteristics of the circuit being described.

C10.3 **Use.** As technology develops, this parameter becomes more archaic and the quality control testing to which this prescribes becomes more machine generated on-line testing and monitoring of specifications. Engineers developing new systems inherently build-in this capability and are no longer expected of the human technical controller to intervene.

C11. CHAPTER 11. PURPOSE AND USE CODE

C11.1 **General.** The Purpose and Use Code (P&U), as indicated, identifies the purpose and/or use of which the circuit and/or trunk requirement will be used based on the customer's defined mission.

C11.2 **Definition of Terms.** Two character coding defined and maintained by the Network Services Directorate (NS) based on several customer-based decision matrix and technology-based solutions. For example: Customer requested a Unclassified but Sensitive Internet Protocol Router (otherwise known as NIPRNet) access circuit; the P&U of this type request will be "IP."

C11.3 **Use.** By indicating the correct type, the tools will then filter the required items needed to build the circuit requirement. This code is used with chapters 2, 5, and 14 to generate a circuit identifier that is unique to each customer requirement.

C12. CHAPTER 12. CIRCUIT TIMING

C12.1 **General.** The circuit timing table elements identify specific timing method to be used on designated circuit or trunk. Standard Defense Information Systems Network (DISN) provided timing is synchronous. Some customer provided equipment requires separate timing sources to keep the data flow moving with minimum errors, this would be referred to as "customer provided" or "external timing."

C12.2 **Definition of Terms.** Circuit timing refers to capability to retain synchronized data transfers between end devices or applications.

C12.3 **Use.** Aides in the determination of timing source to be used for the circuit or trunk requirement.

C13. CHAPTER 13. CLASSIFICATION LEVEL

C13.1 **General.** The classification level describes the security classification to which the specific order pertains. Special rules are associated with distribution of other than unclassified and can be found within security classification guides (under separate cover).

C13.2 **Definition of Terms.** N/A

C13.3 **Use.** N/A

C14. CHAPTER 14. COMMAND COMMUNICATIONS SERVICE DESIGNATOR

C14.1 **General.** The command communications service designator (CCSD) provides a unique eight character identifier for each single service including both circuits and trunks. The first four characters (as defined below) identify who the circuit belongs to, the purpose of the circuit, and the type of service being ordered. The last four characters are machine generated dependent upon region, customer, and other possible rule sets. Table management of the first four characters within the Order Entry and Order Management systems falls under DISA control processes. The day-to-day normal order of listings for authorized CCSDs is based on using an alphanumeric sequence of the last four characters.

C14.2 **Definition of Terms.**

C14.2.1 First Character. Agency Code (Chapter 5)

C14.2.2 Second and Third Character . Purpose and Use (Chapter 11)
(Note: some combinations of Purpose and Use codes with other codes then make the document classified.)

C14.2.3 Fourth Character. Type of Service (Chapter 2)

C14.2.4 Last four characters. For circuits ordered through DISA, this is a system generated group. There are groupings within the full role of possible characters that have been specifically designated for specific Agencies, DISA activities, or Services.

C14.3 **Use.** The CCSD is used in day-to-day communications between users, technicians, Network Operation Centers (NOCs), management, management reports, etc., for identifying circuits and/or trunks under discussion. Many reports and metrics focus on CCSDs when parameters of the reports or metrics are not within scope or /standard.

C15. CHAPTER 15. COMMUNICATIONS SERVICE AUTHORIZATION

C15.1 **General.** The Communications Service Authorization (CSA) is the procurement identifier assigned as part of leasing agreement between Defense Information Technology Contracting Organization (DITCO) and vendors providing service. The DITCO assignment of the CSA will be machine generated using DITCO provided rules. Primary DISA provided tools will be on the receiving end of this data and will make accommodations for data field sizing to ensure the Operations Support System (OSS) portal view to the customer is retrievable and factual.

C15.2 **Definition of Terms.** N/A

C15.3 **Use.** In addition to the above mentioned applicability, the CSA is used within the Chief Financial Executive Directorate (CFE) to differentiate costs per circuit via Telecommunications Inventory Billing Information (TIBI). In the operational environment, the CSA will cross-walk to a vendor provided identifier to which the Network Operations Centers (NOCs) can relay outages or decrease in circuit reliabilities. Telecommunications vendors are required to identify commercial circuits by CSA number, when in discussion with DITCO, or commercial circuit ID(s), when in discussion with NOCs.

C15.4 **Responsibility.** The Office of Primary Responsibility (OPR) for management control and operational direction required to maintain the files is Headquarters, DISA, Procurement Directorate (PLD).

C15.5 **Changes.** As detailed in Basic paragraph 5, with added caveat that DISA Network Service Directorate (NS) Program Management Office (PMO) will facilitate change through the PLD change management processes.

C16 – 18 **RESERVED**

(This page intentionally left blank)

C19. CHAPTER 19. DISA AREA NUMBER OR LETTER

C19.1 **General.** To preserve the integrity of the system from possible duplications within other data sets, the globe is divided into regions (as seen in figure F19.1). The continental United States (CONUS) has also been further divided into regions (as seen in figure F19.2). The global regions are depicted by a numerical character while the CONUS regions are depicted with an alpha connotation.

C19.2 **Definition of Terms.** This element is used in conjunction with geographic location (chapter 33) and State and Country code (chapter 51) to identify a unique location.

C19.3 **Use.** In addition to above mentioned definition and description, this element is used as additional filtering of data queries to aid in full capture for multiple arenas and tasks, i.e., regional concerns (Operations), Capacity Management (Sustainment), and Release and Deploy implementations (node relocations) .

Figure F19.1 GLOBAL REGIONS

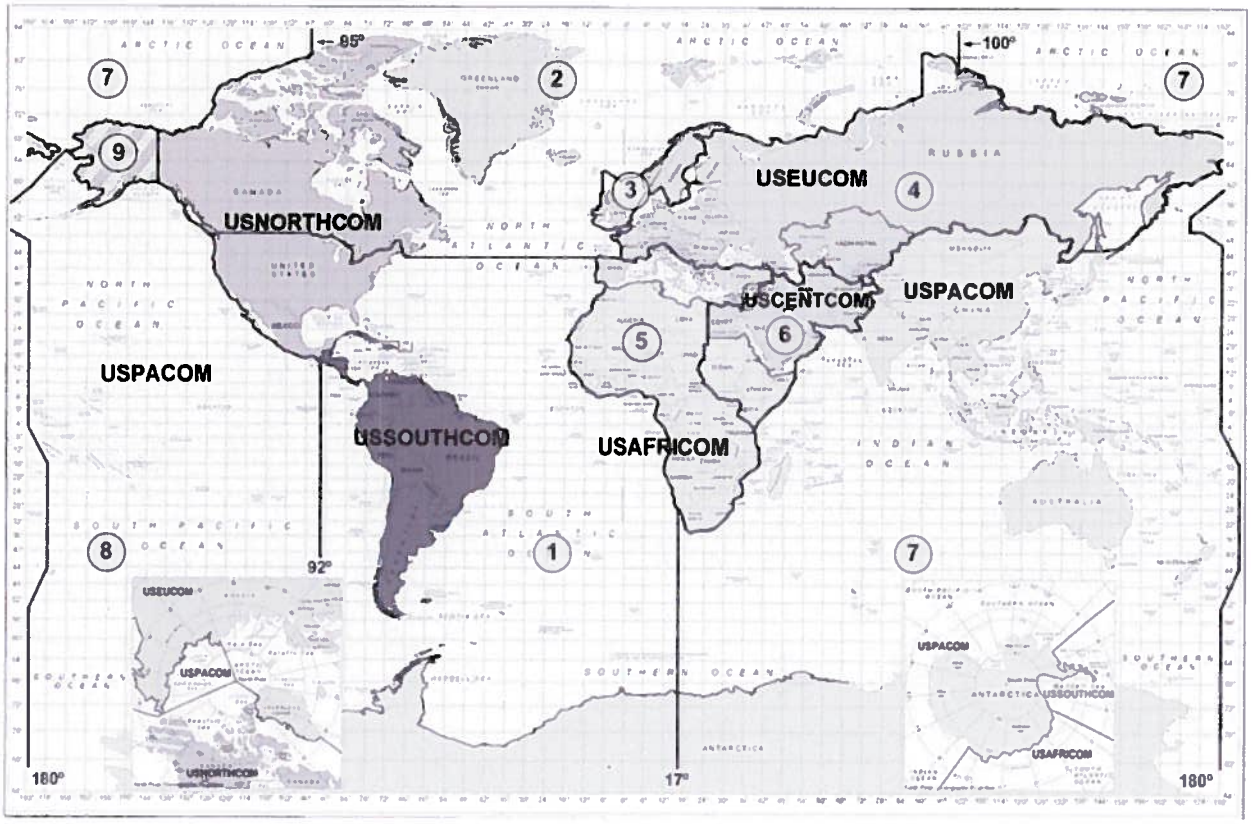
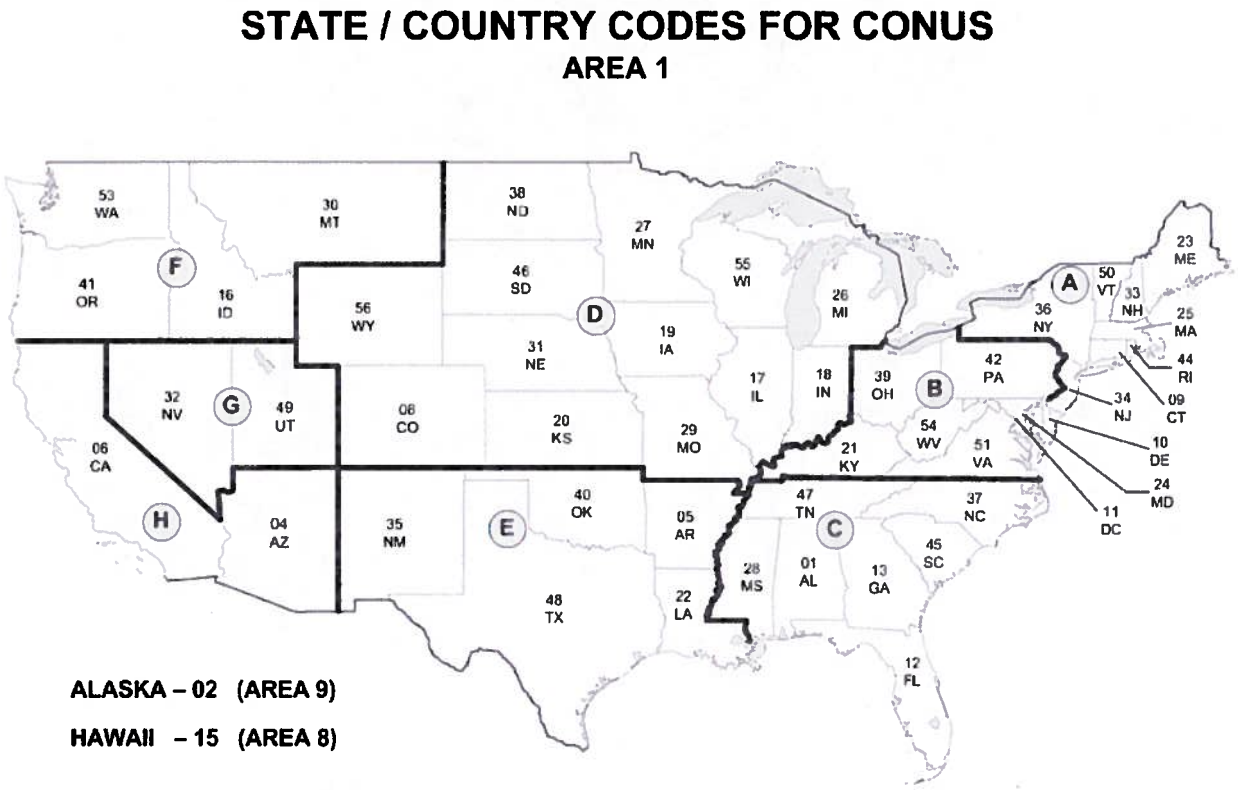


Figure F19.2 CONUS REGIONS



C20. CHAPTER 20. COMPLETION REPORT CODES

C20.1 **General.** The Completion Report is used to notify all concerned as to the status of the circuit's activation. There are four types of Completion Reports, each are defined below with specific description of use being detailed within DISAC 310-130-1, Submission of Telecommunications Requests. With the exception of the In-Effect Report, codes used within the other reports are defined in DISAC 310-130-1 and are available as drop-down options within the tools that assist in the creation of each.

C20.2 **Definition of Terms.**

C20.2.1 **In-Effect Report (IER).** Used to declare circuit fully operational and implemented within the constraints of the issued Telecommunications Service Order (TSO).

C20.2.2 **Exception Report (EXR).** Used to declare the circuit operational; however, engineering or administrative remarks within issued TSO are not exactly as implemented.

C20.2.3 **Delayed Service Report (DSR).** The DSR is used to inform the community of the reason for not meeting the requested operational date in issued order.

C20.2.4 **Ready For Use (RFU).** Used by DISA to inform community that the Defense Information Systems Network (DISN) path has been completed and awaiting customer action to complete the circuit end-to-end.

C20.3 **Use.** Monthly reports are created to inform management of any circuit actions that are completed or delayed due to various reasons. The codes used quickly categorize the problems into areas of responsibility as to who is charged with the action needed to fully activate the circuit requirement.

C21 – 22 **RESERVED**

(This page intentionally left blank)

C23. CHAPTER 23. ENROUTE FACILITY CODES

C23.1 **General.** Enroute facility codes are used to depict the facility or terminal to which the circuit traverses or terminates. Drop down options are available within DISA-provided tools.

C23.2 **Definition of Terms.** In the past, this code was limited to type of facilities in which the equipment was housed, i.e., tech control, commercial relay, etc.. This has now expanded to include type of equipment used to complete the complete path of each circuit requirement.

C23.3 **Use.** The Defense Information Systems Network (DISN) managers use this field to quickly filter circuits to a specific DISN terminal for capacity planning and technical refresh of the DISN technology. This element is also often used by field commands for circuit audits within certain geographical locations.

C24 – 32 **RESERVED**

(This page intentionally left blank)

C33. CHAPTER 33. GEOGRAPHICAL LOCATION

C33.1 **General.** This information describes the geographical location (GEOLOC) of a communication terminal or facility in terms of the established name of the place listed in U.S. Geographical Survey published Gazetteer, Department of Transportation Atlas, Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3150-15E, (U) Standard Specified Geographic Location File Request (GEOREQ), and JOPES (Joint Operations Planning and Execution System) reference files. The content of this table is under constant review and change. It is maintained in an on-line system capacity and no longer maintained in a hard-copy format

C33.2 **Definition of Terms.** Procedures for creating new codes are held within process manager global work instructions.

C33.3 **Use.** GEOLOC is used alongside other filtering elements are used for managers to quickly determine circuit inventory for each site.

C34 – 36 **RESERVED**

(This page intentionally left blank)

C37. CHAPTER 37. MULTIPOINT FLAG

C37.1 **General. A Multipoint flag is** used only for multipoint circuits to identify the circuit terminal locations except for the last terminal and to identify the locations at which the circuit is hubbed to more than one terminal.

C37.2 **Definition of Terms.** N/A

C37.3 **Use.** As identified in C37.1.

C38 **RESERVED**

(This page intentionally left blank)

C39. CHAPTER 39. TELECOMMUNICATION SERVICE PRIORITY AUTHORIZATION CODE

C39.1 **General.** Telecommunication Service Priority (TSP) authorization code identifies the priority levels for both the creation (ordering and activating) and restoration of those requirements customers have received approval from the Department of Homeland Security that meet the National Security Council's defined criticality definitions. It has monetary connotations as it pertains to vendor implementation and restoral (if engineered solution to circuit requirement is provided via Defense Information Technology Contracting Organization (DITCO) contracts).

C39.2 **Definition of Terms.** Detailed guidance is provided in DISAC 310-130-1, Submission of Telecommunication Requests, and DISAC 310-130-4, Defense User's Guide to the Telecommunications Service Priority (TSP) System.

C39.3 **Use.** Application by customer with the Department of Homeland Security will determine the priority level based on short questionnaire. This information is currently outside the DISA process of providing telecommunication requirements but is later inserted manually as part of the final order. This coding is currently only valid within the continental United States (CONUS) for vendor support. Outside CONUS requires other laws and tariff arrangements for priority implementation and restoral.

C40. CHAPTER 40. PROGRAM DESIGNATOR CODE

C40.1 **General.** The program designator code (PDC) identifies the Agency and Program designated and the primary source of funding for the circuit described. Initial creation of such coding is handled under separate Defense Information Technology Contracting Organization (DITCO) processes not defined under this guidance.

C40.2 **Definition of Terms.** The four to six character code is used as primary source of funding unless otherwise designated within the service order.

C40.3 **Use.** As identified above.

C40.4 **Responsibility.** The Office of Primary Responsibility (OPR) for management control and operational direction required to maintain the files is Headquarters, DISA, Chief Financial Executive (CFE) under its subcommand within the DITCO.

C40.5 **Changes.** As detailed in paragraph 7 of the basic Circular with added caveat that DISA Network Services Directorate (NS) Program Management Officer (PMO) will facilitate change through the Procurement Directorate (PLD) change management processes unless otherwise noted.

C41 – 42 **RESERVED**

(This page intentionally left blank)

C43. CHAPTER 43. NATIONAL SECURITY SYSTEM

C43.1 **General.** Identifies a circuit requirement as "national security system" (NSS) or "nonnational security system." If a circuit is NSS, the justification for this requirement is detailed in DISAC 310-130-1, Submission of Telecommunications Requests. This is a two-character code, with first character answering either "Y" (yes) for NSS or "N" (no) for non-NSS. The second character only applies if first character is "Y." Term and codes included herein due to recent change to add code "Y6." This is a customer option from a drop-down menu within order entry.

C43.2 **Definition of Terms**

C43.2.1 When combined with "Y," the justification is as described as follows:

C43.2.1.1 Y1. Requirement involves intelligence activities.

C43.2.1.2 Y2. Requirement involves cytological activities related to national security.

C43.2.1.3 Y3. Requirement involves command and control of military forces.

C43.2.1.4 Y4. Requirement involves equipment that is an integral part of a weapon or weapon systems.

C43.2.1.5 Y5. Requirement is critical to the direct fulfillment of military or intelligence missions. A system is not a NSS if it is used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

C43.2.1.6 Y6. Requirement is critical to the classified communications capability.

C43.3 **Use.** Identification of those requirements requiring special support and/or oversight.

C43.4 **Responsibility.** The Office of Primary Responsibility (OPR) for management control and operational direction required to maintain the files is Headquarters, DISA, Network Services Directorate (NS). Changes or additions to this element will require coordination with the Joint Staff and Office or the Secretary of Defense.

C44 – 45 **RESERVED**

(This page intentionally left blank)

C46. CHAPTER 46. SECURITY EQUIPMENT

C46.1 **General.** If needed, this data element will identify the security status or the security equipment to be used in implementing a circuit requirement. The DISA order entry tools allow for a drop-down menu available for which customers can choose the security equipment to use in implementation. The listed types are a part of the DISA Approved Product List (APL) for use on the Defense Information Systems Network (DISN).

C46.2 **Definition of Terms.** Cryptological equipment is any cipher or decipher capable equipment to prevent data being disclosed to parties to which it was not intended.

C46.3 **Use.** This element allows for quick by-type-filtering for any/all circuit requirements.

C47 – 48 **RESERVED**

(This page intentionally left blank)

C49. CHAPTER 49. SERVICE AVAILABILITY

C49.1 **General.** Indicates when or how the circuit, trunk, or link is made available for the designate user.

C49.2 **Definition of Terms.** This term and subsequent use is technology driven along with end-user requirement of transmission.

C49.3 **Use.** DISN standard is "full period."

C50 **RESERVED**

(This page intentionally left blank)

C51. CHAPTER 51. STATE AND COUNTRY CODE

C51.1 **General.** Identifies the state or country associated with a geographical location (GEOLOC). This element is database controlled by DISA and is used in conjunction with chapter 33 to identify a specific location globally.

C51.2 **Definition of Terms.** Multiple locations worldwide may have the coincidental circumstances of being named the same; this element control is to aid in the distinctiveness of each site supported.

C51.3 **Use.** While used in conjunction with geographic location, it can also be used to filter requirements within specific regions.

C52 – 53 **RESERVED**

(This page intentionally left blank)

C54. CHAPTER 54. TELECOMMUNICATIONS SERVICE REQUEST NUMBER

C54.1 **General.** The Telecommunications Service Request (TSR) number identifies the Agency and/or Department to which certification authority resides, date (DDMMMYY), and sequential numeration giving the requirement a distinct traceable identifier.

C54.2 **Definition of Terms.** Within DISA provided tools, this number is managed internally by the system based on policy set forth within DISAC 310-130-1, Submission of Telecommunications Requests. Normally, a 13-alphanumerical sequence, based on the above definition, other actions may necessitate the inclusion of an additional alpha character to the sequence to delineate amendments, cancellation, etc., from the original basic document.

C54.3 **Use.** Used to accurately identify and enable tracking of each requirement from customer submission to fulfillment of that requirement. Process delineates methodology for practice amongst the DISA activities as to which customer coded requirements are worked within which activity.

C55. CHAPTER 55. TELECOMMUNICATIONS SERVICE ORDER NUMBER

C55.1 **General.** The Telecommunications Service Order (TSO) number identifies the DISA activity originating the requirement, the year it was issued, its sequential position among those issued within that year by that activity, and the number of ordered actions against the described circuit.

C55.2 **Definition of Terms.** Within DISA, two organizations provide the service to which this applies and process manager level agreements are in place to delineate how the first letter coding is to be defined.

C55.3 **Use.** Used to describe the circuit from an end-to-end perspective and to give authorization (order) to proceed with any purchases on behalf of the customer to fulfillment.

C56 – 88 **RESERVED**

(This page intentionally left blank)

C89. CHAPTER 89. TYPE OF ACTION CODES

C89.1 **General.** The type of action code is used by the customer to differentiate what their request is to do. These options are detailed within DISAC 310-130-1, Submission of Telecommunications Requests, and DISA-provided tools will allow for menu-driven associations to create the Telecommunications Service Request (TSR). Changes to the options with full justification are to be worked through the Request Fulfillment Process Owner who will communicate the request after validation to the tool architects for changes to the DISA-provided tools.

C89.2 **Definition of Terms.** As defined above.

C89.3 **Use.** Primary use is to identify actions to take regarding the requirement. May also be used as a management filtering capability.