



Defense Information Systems Agency

**A Combat Support Agency**

# **NETWORK SERVICES**

## **VIRTUAL PRIVATE NETWORKS**

### **ESTABLISH A VIRTUAL PRIVATE NETWORK (VPN)**

#### **CUSTOMER ORDERING GUIDE**

Version 3.1  
October 02, 2013

**UNCLASSIFIED**

Network Services  
P.O. Box 549  
Ft. Meade, MD 20755-0549

This page intentionally left blank.

## Signature Page for Key Officials

*Approved by:*

*Matthew Q. Breen*

Chief, Customer Services Division (NSP4)

*02 Oct 2013*

Date

This page intentionally left blank.

## Revision History

Version Number	Date	Summary of Changes	Org
1.0	July 2, 2012	Initial release.	NS7
2.0	November 14, 2012	Revised to include a variety of new VPN services and future VPN services. Document renamed and changed to focus on providing guidance and steps to order various VPN services.	NS7
2.1	January 15, 2013	Revised to include differences in ordering associated with Private ISP Service and IAP Gateway at DECC.	NSP4
2.2	January 25, 2013	Added DTEN type available now. Ensure references consistent throughout doc. Updated acronyms.	NSP4
2.3	March 07, 2013	Added NIPRNet Federated Gateway.	NSP4
2.4	March 12, 2013	Updated links to Enterprise Connection. Prepared for release to external mission partners.	NSP4
2.5	May 06, 2013	Update to add availability of MED COI and CMNT COI.	NSP4
3.0	August 14, 2013	Update to note DGSC email address change, change name from DTEN to DTES, add availability Quality of Service (QOS), and provide information for Private Data ISP Service IP address space requirements.	NSP4
3.0	September 06, 2013	Final review edits	NSP4
3.1	October 02, 2013	Update note on DTES CNDSP.	NSP4

# Table of Contents

<b>1. Introduction.....</b>	<b>8</b>
<b>2. Purpose.....</b>	<b>9</b>
<b>3. References.....</b>	<b>9</b>
<b>4. Roles and Responsibilities .....</b>	<b>9</b>
<b>5. Points of Contact.....</b>	<b>9</b>
<b>6. VPN Services Descriptions.....</b>	<b>10</b>
6.1 Private IP Service (Layer 3 VPN).....	10
6.2 Private LAN Service (Layer 2 VPN).....	10
6.3 Label Transport Service (Layer 2 VPN).....	10
6.4 DISN Test and Evaluation Service (DTES – Layer 3 VPN).....	11
6.5 Secret Private IP Service (Classified Layer 3 VPN).....	11
6.6 Private Data ISP Service (Layer 3 VPN).....	11
6.7 Internet Access Point (IAP) Demilitarized Zone (DMZ) (Layer 3 VPN) .....	12
6.8 Mission Partner Gateway (MPG)/NIPRNet Federated Gateway (MPG/NFG) Community of Interest (COI) (Layer 3 VPN).....	12
6.9 CMNT COI (Layer 3 VPN).....	13
6.10 Med COI Service for integrated Electronic Health Records (iEHR) (Layer 3 VPN)...	14
<b>7. Process Overview .....</b>	<b>14</b>
<b>8. Business Rules .....</b>	<b>15</b>
<b>9. Steps to Establish a VPN on DDOE .....</b>	<b>17</b>
<b>10. Other Action Requests – VPNs.....</b>	<b>25</b>
<b>Appendix A Acronym List.....</b>	<b>27</b>

## List of Illustrations

<b>Table 1: VPN Services .....</b>	<b>8</b>
<b>Table 2: Points of Contact.....</b>	<b>10</b>
<b>Figure 1: Process to Establish a VPN.....</b>	<b>15</b>
<b>Figure 2: Type of Service Page .....</b>	<b>18</b>
<b>Figure 3: Request Action Page.....</b>	<b>18</b>
<b>Figure 4: General Information Page.....</b>	<b>20</b>
<b>Figure 5: Establish a VPN Information Page.....</b>	<b>21</b>
<b>Figure 6: Example of Submitted Request Summary Page – Top Half .....</b>	<b>23</b>
<b>Figure 7: Example of Submitted Request Summary Page – Bottom Half.....</b>	<b>24</b>
<b>Figure 8: Example of Auto-Generated E-mail of Approved Request to Establish a VPN..</b>	<b>25</b>
<b>Figure 9: Request Action Page for Other Actions .....</b>	<b>26</b>

# 1. Introduction

The Defense Information System Network (DISN) continues to support and deploy Virtual Private Network (VPN) services. VPN technologies provide agile networking within communities of interest over the common Internet Protocol (IP) network, and enable users to migrate away from inefficient dedicated circuit private networks. As data services, these new services fall within the DISN Subscription Service (DSS) structure. This document addresses the ordering of the VPN services available either now or in the near future. It also announces the implementation of Quality of Service (QOS) for specific VPN service types. The VPN services and VPN codes are listed in Table 1. Detailed service descriptions are provided in Section 6.

The process and detailed information to order these services, which requires two steps, are provided in these VPN Ordering Guides. The first step is to **Establish a VPN** and the second step is to **Connect to an Established VPN**. Guidance for registering VPNs in the System/Network Approval Process (SNAP) database is provided in the VPN SNAP Registration Process Guide available at: <http://disa.mil/Services/Network-Services/Notices>. In addition, the appendices of the Connection Process Guide (GPC) also provide registration of VPN services in SNAP. The electronic or print copy of the CPG can be accessed at: <http://www.disa.mil/Services/Network-Services/Enterprise-Connections/Connection-Process-Guide>. For registration of VPN services in the SIPRNet GIG Interconnection Approval Process (GIAP) System (SGS) database, visit <https://www.disa.smil.mil/connect> via Secret Internet Protocol Router Network (SIPRNet).

VPN Code	Service Names
L3	Private IP Service (Layer 3 VPN)
L2	Private LAN Service (Layer 2 VPN)
CX	Label Transport Service (Layer 2 CsC VPN)
TE	DISN Test & Evaluation Service (DTES – Layer 3 VPN)
DKL300251	Medical Community of Interest for integrated Electronic Health Records (iEHR) (Med COI – Layer 3 VPN) - <i>Authorized “Medical Community Only” users of the Department of Defense (DoD) and Department of Veterans Affairs (VA) use only. Customers can ONLY submit “Connect to an established VPN” requests for this service. DISA Control Number (DCN) code for this service is D314.</i>
DKL342000	Common Mission Network Transport (CMNT) Community of Interest (CMNT COI – Layer 3 VPN) - <i>Customers can ONLY submit “Connect to an established VPN” requests for this service</i>
DKL300227	Private Data ISP Service (formerly known as Private ISP Service) (All Customers – Layer 3 VPN) - <i>Customers can ONLY submit “Connect to an established VPN” requests for this service</i>
C3	Secret Private IP Service (Classified Layer 3 VPN)
DOL300230	IAP DMZ (All Customers – Layer 3 VPN) - <i>Customers can ONLY submit “Connect to an established VPN” requests for this service</i>
DKL300249	MPG/NFG COI (All Customers – Layer 3 VPN) ) - <i>Customers can ONLY submit “Connect to an established VPN” requests for this service</i>

**Table 1: VPN Services**

**Note: More VPN codes may be added in the future.**

All VPN services are available now for ordering via DISA Direct Order Entry (DDOE ) with the following exceptions: C3, Secret Private IP Service (Classified Layer 3 VPN); DOL300230, Internet Access Point (IAP) Demilitarized Zone (DMZ) (All Customers – Layer 3 VPN); DKL300249, Mission Partner Gateway/NIPRNet Federated Gateway Community of Interest (MPG/NFG COI) (All Customers – Layer 3 VPN); and the DKL300227, Private Data ISP Service (All Customers – Layer 3 VPN). These remaining VPN services will be available within the next Fiscal Year (FY) 2014. A DISN Business Service Catalog (BSC) Customer Notice and an announcement will be posted to the DISA Direct homepage, announcing the availability of these services, which can be accessed at:

<https://www.disadirect.disa.mil/products/ASP/welcome.ASP>.

## 2. Purpose

This document provides detailed information necessary to **Establish a VPN** via DISA Direct Order Entry (DDOE) for available VPN Services noted in the table above. It includes minor differences in ordering associated with Private Data ISP Service, Internet Access Point (IAP) Demilitarized Zone (DMZ), Common Mission Network Transport (CMNT) Community of Interest (COI) (now Layer 3 only), Medical Community of Interest for integrated Electronic Health Records (iEHR) (Med COI – Layer 3 VPN), and Mission Partner Gateway (MPG)/NIPRNet Federated Gateway (NFG) Community of Interest (COI) VPN services. A separate Ordering Guide has been developed to address information to **Connect to an Established VPN**. Both documents assume the reader has basic familiarity with DDOE and has an established account with role(s). The DISA Direct homepage can be accessed at the link provided above.

## 3. References

- (a) DoD Connection Process Guide (CPG), Version 4.3, dated May 15, 2013

## 4. Roles and Responsibilities

It is the customer's responsibility to order VPN services, as they deem necessary, and to ensure the registration within the SNAP and the SGS databases.

## 5. Points of Contact

For additional information, help with DDOE, or specifically with ordering VPN services, contact the DISN Global Support Center (DGSC) using the information provided below.

DISN Global Support Center (DGSC)	
Customer Services Division (NSP4)	DSN: (510) 376-3222 or (312) 850-4790 CML: (800) 554-3476 or (614) 692-4790 SBU IP Data e-mail: <a href="mailto:DISA.DGSC@MAIL.MIL">DISA.DGSC@MAIL.MIL</a> Secret IP Data e-mail: <a href="mailto:DGSC@COLS.CSD.DISA.SMIL.MIL">DGSC@COLS.CSD.DISA.SMIL.MIL</a>

Table 2: Points of Contact

## 6. VPN Services Descriptions

### 6.1 Private IP Service (Layer 3 VPN)

This VPN service enables customers to reduce circuit, equipment, and accreditation paperwork costs for data transfer and enclave connectivity using the DISN as transport. DISN Private IP Service is an enterprise VPN service providing data privacy to customers across the DISN. This service is available as part of the DSS Cost Recovery Model at any DSS location that includes Sensitive but Unclassified Internet Protocol Data (SBU IP Data) Service. Private IP service will enable customers to migrate from Asynchronous Transfer Mode (ATM) to IP by using this Layer 3 VPN service, and provide segmented data transport across the IP network to connect enclaves without dedicated circuits. The Information Assurance (IA) and Connection Approval Process (CAP) accreditation is significantly faster and requires less paperwork to complete. This service provides a segmented IP service for customers utilizing a Multiprotocol Label Switching (MPLS) Layer 3 VPN, and it requires a separate physical interface for each connection.

### 6.2 Private LAN Service (Layer 2 VPN)

This VPN service provides customers the ability to shrink the world to one Local Area Network (LAN) regardless of their physical location around the world. Private LAN service is a way to provide Ethernet based multipoint-to-multipoint communication over the DISN IP MPLS network. This allows geographically dispersed sites to share an Ethernet broadcast domain by connecting sites through pseudo-wires. This layer 2 VPN technology allows any-to-any (multipoint) connectivity. The LAN at each site, is extended to the edge of the DISN. The network emulates a switch/bridge to connect all of the customer LANs to create a single bridged LAN. It provides a segmented IP service for customers utilizing an MPLS Layer 2 VPN.

NOTE: This new service is dependent on acquisition and installation of IP Transport Provider Edge (IPT-PE) router infrastructure and it requires a separate physical interface.

### 6.3 Label Transport Service (Layer 2 VPN)

This VPN service enables customers to reduce long haul expenditures using IP as transport for data. It is a Layer 2 VPN routing based on MPLS label. This service is available as part of the DSS Cost Recovery Model at specific locations. It is an alternative service for some ATM and Low-Speed Time Division Multiplexing (LSTDM) customers. It provides a segmented IP service for customers utilizing an MPLS Layer 2 VPN.

NOTE: This new service is dependent on acquisition and installation of IPT-PE router infrastructure and it requires a separate physical interface.

## **6.4 DISN Test and Evaluation Service (DTES – Layer 3 VPN)**

Test and Evaluation (T&E) IP data (operating over the DTEN, known as DISN Test & Evaluation Network) is part of the DSS Cost Recovery Model. This VPN service provides a BLACK transport capability riding the DISN Backbone. It offers standard DISN services and Service Level Agreements (SLAs) to DTES customers. The Communities of Interest (COIs) are responsible for their Computer Network Defense Service Provider (CNDSP) services. This is out of DISA's Management Boundaries. DISA will not be responsible for COIs customers' CNDSP nor for customers' Communications Security (COMSEC).

## **6.5 Secret Private IP Service (Classified Layer 3 VPN)**

This VPN service enables customers' classified data the same opportunity to reduce costs as their unclassified data. Secret Private IP Service is an enterprise VPN service providing data privacy to customers across the Secret IP Data Service. This service is available as part of the DSS Cost Recovery Model at any DSS location that includes Secret IP Data Service. In addition, it provides a segmented IP service for customers utilizing an MPLS layer 3 VPN, and requires a separate physical interface for each connection.

## **6.6 Private Data ISP Service (Layer 3 VPN)**

This VPN service (formerly known as Private ISP Service) provides customers the ability to obtain internet access through an MPLS layer 3 VPN at any DISN Internet Access Point (IAP). Private Data Internet Service Provider (ISP) Service is an enterprise VPN service providing ISP access to customers across the DISN. This service is available as part of the DSS Cost Recovery Model at any DSS location that includes SBU IP Data Service. Connection Approval Process (CAP) accreditation is significantly faster and requires less paperwork to complete. A separate physical interface is required.

This VPN is “established” by DISA NS. Customers can ONLY submit Telecommunications Requests (TRs) in DDOE to “connect to an established VPN”, VPN Identifier: DKL300227.

In addition, customers will be required to request IP Address space from the DoD Network Information Center (NIC) for their connection to work in the Private Data ISP Service. Customers must obtain the IP Address Space out of the reserved IP space for Private Data ISP Service: 139.241.0.0/16. Reference the *Connect to an Established VPN Customer Ordering Guide*, Business Rule #5, for IP address space block information and instructions.

## **6.7 Internet Access Point (IAP) Demilitarized Zone (DMZ) (Layer 3 VPN)**

This VPN service provides customers the ability to obtain internet access through an MPLS layer 3 VPN at any Defense Enterprise Computing Center (DECC) location to access any DISN IAP. It is an enterprise VPN service providing IAP internet access to customers across the DISN. This service is available as part of the DSS Cost Recovery Model at any DSS location that includes SBU IP Data Service. Customers must use DCN, D316 when submitting requests to connect to this service.

This VPN is “established” by DISA NS. Customers can ONLY submit Telecommunications Requests (TRs) in DDOE to “connect to an established VPN”, VPN Identifier: *DOL300230*.

## **6.8 Mission Partner Gateway (MPG)/NIPRNet Federated Gateway (NFG) Community of Interest (COI) (Layer 3 VPN)**

The Department of Defense (DoD) has granted some non-DoD federal agencies and mission partners connections directly into the SBU IP Data Service. This introduces a potential threat to the SBU IP Data Service due to the absence of any mechanisms for effectively controlling and monitoring traffic to/from these agencies. The path forward is to acquire and deploy Mission Partner Gateways (MPG)/NIPRNet Federated Gateways (NFG) at multiple IAP locations to provide a secure and robust means for these agencies to connect to the SBU IP Data Service. The benefit is that it will provide protection from and visibility into threats and events involving traffic to/from these agencies and partners. MPG/NFG shall support customers using physical/logical connections (described below as “External Customer Connecting Directly to NFE Router” and “External Customer on SBU IP Data Service”). The system shall support logical traffic separation as traffic transits through SBU IP Data Service.

This service is for non-DoD federal agencies and mission partner connections that connect directly into the SBU IP Data Service. Customers ordering this service will be connected to the DISN but will have their connection directed to the nearest MPG/NFG External (NFE) router. All traffic will go through the NFE prior to accessing any DoD available networks.

MPG/NFG customers can be categorized into two types:

1. External Customer Connecting Directly to NFE Router. The first and simplest type of connection is directly to the NFE router. The benefit is to keep the non-DoD partner traffic separate from the IAPNet infrastructure. These mission partners may connect to the NFE router via third-party leased circuit or transport provided by DISN transport infrastructure. It is also possible that the customer equipment may be collocated with an MPG/NFG site and with back-to-back connections with the router. With these types of connections, encryption may not be necessary. These customers may use External Border Gateway Protocol (eBGP) peer directly with the NFE router over the physical circuit using interface an Internet Protocol (IP) address.

2. External Customer on SBU IP Data Service. The second type is a mission partner currently connecting directly to SBU IP Data Service. This type of customer sometimes has their own back-end connection to the Internet. The goal of this MPG/NFG design is to leverage the existing connections to SBU IP Data Service without installing new circuits. This can be accomplished by providing a physical trunk between the NFE and the collocated Unclassified Provider Edge (UPE) router. A partner may build a logical tunnel, possibly encrypted, to the NFE router over this physical connection. This encryption will be broken between the NFE and MPG/NFG Internal (NFI) for inspection/monitoring. The customer router will no longer have BGP peering directly with the UPE/Aggregation Router (AR) router, but instead exchange eBGP routes only with the NFE router over the tunnel. Additionally, a new MPLS Layer 3 VPN (L3VPN) (e.g., NFE\_VPN) has been created to isolate traffic for these customers from the rest of SBU IP Data Service to sense traffic before the NFE and IA components inspect it. The NFE routers from all MPG/NFG sites would also be members of this VPN and are visible to all these customer routers. An external customer on this VPN may peer with multiple NFE routers for redundancy. Tunnel and encryption between customer routers and the NFE router is optional and can overlay the VPN.

The VPN Naming Convention was used to obtain the VPN ID for the MPG/NFG Community of Interest (COI). The VPN ID for the MPG/NFG COI service is provided by DISA and will always be the same for every mission partner.

This VPN is “established” by DISA NS. Customers can ONLY submit Telecommunications Requests (TRs) in DDOE to “connect to an established VPN”, VPN Identifier: *DKL300249*. Customers must use DCN, D212 when submitting requests to connect to this service.

## 6.9 CMNT COI (Layer 3 VPN)

The Common Mission Network Transport (CMNT) COI provides a distinct and common transport for Combined Enterprise Regional Information Exchange System (CENTRIXS) traffic in order to meet mission partners’ multi and bilateral communication requirements. Simply put, CMNT will separate the CENTRIXS coalition networks (enclaves) from the Secret IP Data Service, thereby eliminating CENTRIXS’ dependence upon Secret IP Data Service for transport. This requirement supports DoD Instruction 8110.1 guidance of integrating CENTRIXS and other operational Mission-Partner networks into existing DoD general service communications infrastructure as separate networks servicing all DoD Mission Partner information sharing requirements.

This VPN service provides CMNT customers the ability to obtain Community Of Interest (COI) access through an MPLS layer 3 VPN at any DISN DSS location that includes IPT-PE IP Data access. CMNT VPN Service is an enterprise VPN service providing mission partners’ access to customers across the DISN. This service is available as part of the DSS Cost Recovery Model at any DSS location that includes IPT-PE IP Data access. Connection Approval Process (CAP) accreditation is significantly faster and requires less paperwork to complete. A separate physical or logical interface is required to implement this service.

The VPN naming convention was used to obtain the VPN ID for CMNT VPN service. The VPN ID for the CMNT VPN service is provided by DISA and will always be the same for every CMNT customer. Coalition Mission Network Transport VPN Service VPN ID: *DKL342000*. DDOE will assign this VPN ID to all CMNT customers requesting CMNT VPN Service.

NOTE: CMNT VPN service is a “Mission Partner / COCOM only” service. Customers ordering this service will be connected to the DISN but will not have access to the World Wide Web, SBU IP Data Service, or Secret IP Data Service. No access to DoD networks is available. This is a restricted access service and all requests to connect to this service will be verified and approved by DISA.

Customers can ONLY submit Telecommunications Requests (TRs) in DDOE to “connect to an established VPN”, VPN Identifier: *DKL342000* for CMNT COI (Layer 3 VPN).

## **6.10 Med COI Service (Layer 3 VPN) for integrated Electronic Health Records (iEHR)**

The Medical Community of Interest (Med COI) service for integrated Electronic Health Records (iEHR) is a VPN service that provides customers the ability to connect to the Med COI through an MPLS layer 3 VPN. Med COI is an enterprise VPN service providing access to the Medical Community of Interest VPN for authorized users of the Department of Defense (DoD) and Department of Veterans Affairs (VA). DoD and/or VA Med COI approving authority can only authorize connection to this VPN. This service is available as part of the DSS Cost Recovery Model at any DSS location that includes SBU IP Data Service. Connection Approval Process (CAP) accreditation is required and the process is significantly faster and requires less paperwork to complete. Use of a virtual interface is approved but not required.

The Med COI for integrated Electronic Health Records (iEHR) VPN has been established under the authority of the Secretary of Defense ACTION MEMO dated 25 Feb 2013. This is part of the integrated Electronic Health Record (iEHR) initiative between the DoD and VA.

The VPN ID for the Med COI service is provided by DISA and will always be the same for every customer. Med COI Service for integrated Electronic Health Records (iEHR) VPN ID: *DKL300251*. DDOE will assign this VPN ID to all customers requesting Med COI Service.

NOTE: Med COI service is a “Medical Community Only” service. Customers ordering this service will be connected to the DISN but will only have access to the Med COI enclave set up between DoD and VA. No access to DoD or VA networks is available.

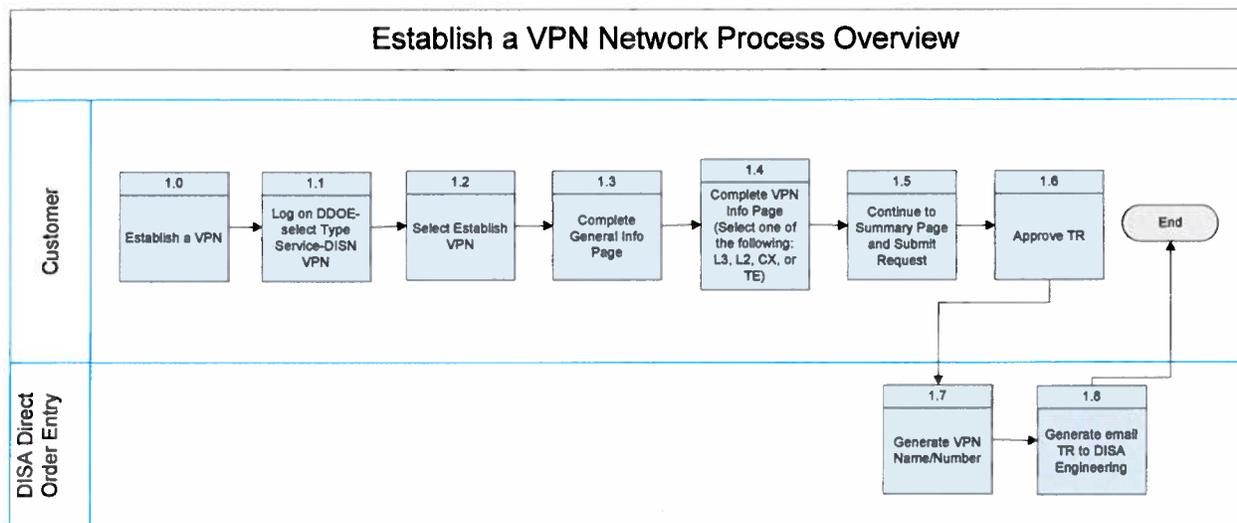
Customers can ONLY submit Telecommunications Requests (TRs) in DDOE to “connect to an established VPN”, VPN Identifier: *DKL300251* for Med COI Service for integrated Electronic Health Records (iEHR) (Layer 3 VPN). DISA Control Number (DCN) code for this service is D314. DDOE will automatically populate all Med COI orders with this DCN number.

## **7. Process Overview**

The process to establish a VPN is required only once for each VPN type (L2, L3, CX, TE) regardless of the number of individual connections. This is an administrative action/record only; it does not result in the issuance of a Telecommunications Service Request (TSR) or Telecommunications Service Order (TSO). The basic procedures are:

1. The DDOE process is used to establish a VPN.
2. An authorized DDOE user logs into DDOE and selects type of service [i.e., DISN Virtual Private Network (VPN)] and “Establish a Virtual Private Network (VPN).”
3. A VPN Point of Contact (POC) will be designated. An Alternate POC may also be designated.
4. A VPN Name/Number will be generated by DDOE according to DISAC 310-65-1 naming convention rules. Customers will receive feedback indicating successful action and providing the VPN Name/Number to be used when ordering connections.

The following depicts the process overview for establishing a VPN. Business rules and specific steps are documented in subsequent sections.



**Figure 1: Process to Establish a VPN**

## 8. Business Rules

Ordering of the DISN VPNs is based on the basic premise and template for ordering the Sensitive but Unclassified (SBU) IP Data service. Additional business rules apply when ordering these services.

1. All DISA Direct users that have the role of Authorized Requesting Official (ARO) or DISA users that have the role of Authorized Provisioning Official (APO) will have the capability to select DISN VPNs as the type of service.

2. The action types that apply to **Establish a VPN** are: Establish a VPN, Change VPN Point of Contact (POC) Information, and Discontinue a VPN. These actions are performed on the VPN (network) itself, vice individual connections to the established VPN. The following rules apply when establishing a VPN. This action type is NOT available for Private Data ISP Service, IAP DMZ, CMNT COI, Med COI, and MPG/NFG COI VPN type services. See sections 6.6, 6.7, 6.8 6.9, and 6.10.
  - a. Funding requirements are IAW the business rules for the DISN Subscription Services (DSS) cost recovery model.
  - b. No Telecommunications Service Request (TSR) will be generated.
  - c. An e-mail is sent to applicable engineering e-mail address/originator/all Point of Contacts (POCs), and any added e-mail addresses upon final approval of the Telecommunications Request (TR). The action e-mail address of the engineering e-mail is based upon the geographical disposition selection made on the Establish a VPN TR.
  - d. The full VPN Identifier (ID) will be automatically generated upon final approval of TR. This identifier will be needed in order to submit requests to connect to the established VPN.
  - e. TR routing for this type of request is based upon a new routing identifier – VPN Routing ID. The setup and maintenance will be part of the Request Routing application and the responsibility of the Agency's Routing List Official (RLO).
  - f. To discontinue an established VPN (network), all individual physical VPN connections to that network must be disconnected first.
  - g. The Agency's Routing List Official (RLO) utilizes the Request Routing application to setup and maintain the VPN Routing ID. All of the agency's VPN Routing IDs that have been setup by the RLO are automatically presented on the TR page for selection when establishing a VPN.
  
3. Quality of Service (QOS) Implemented - QoS is 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 give one customer's traffic a higher priority than another customer's traffic.

For Example: There are two customers that have both "Real Time" (video) and "Scavenger" (low priority data) traffic being processed by the same node/interface. If their communication link becomes congested, the two customers will both lose their "Scavenger" traffic but both will retain their "Real Time" traffic.

Effective immediately, the Telecom Request (TR) will auto-populate the type of QOS template. The following type service offerings will reflect QOS General Transport Path (GTP): DISN Virtual Private network (VPN) (Private IP Service (Layer VPN) - L3, Private LAN Service (Layer 2 VPN) - L2, and Label Transport Service (Layer 2 CsC) - CX). The QOS template code

will automatically be reflected in TSR Item 142. Service offerings not listed here, will not reflect QOS.

## 9. Steps to Establish a VPN on DDOE

This section provides steps necessary to establish a VPN. All the steps and screens for establishing a VPN are the same for all the VPN service types (L2, L3, CX and TE). The only difference is in selecting the “type of VPN” in the Virtual Private Network Information Page. The examples provided are specifically for the L3 - Private IP Service (Layer 3 VPN).

Private Data ISP Service, IAP DMZ, CMNT COI, Med COI, and MPG/NFG COI are DISA NS established VPNs. Customers cannot establish these VPN types but can ONLY request connections to the DISA NS established VPN types. See sections 6.6, 6.7, 6.8, 6.9, and 6.10.

**ACTION:** ARO/APO selects “DISN Virtual Private Network (VPN)” as the service type as shown below, and clicks “Continue.” APO role is a DISA staff ONLY role.

**Type of Service Page**

[DISA Direct Home](#)   [Notifications](#)   [TR Home](#)   [TR Help](#)   [Track TR](#)   [CAD](#)   [ABD](#)

**WARNING!** Use of the Back and Forward buttons on the browser may cause undesired results, therefore they should NOT be used to navigate through the request.

**TR Notice:** When a TR is created, a Customer Job Order Number (CJON) will be automatically assigned to the request using the following format (“WO” followed by day, month, year, and next sequential number (e.g., WO20APR011234)). Also, based on DISAC 310-130-5, table T1.1 the Web will assign a TCO code to the request. Once the request has been approved by the final approver within the routing matrix and forwarded to DISA for action, the Web will assign a TR number using the TCO code previously assigned and the same format as the “WO” number. The CJON and TR numbers will be passed back electronically to everyone in the approval chain. Both numbers will also be reflected on the output document.

**Please select the Type of Service:**

? **(M)** Type of Service:

**DISCLAIMER!** The final solution to your telecommunication requirement will be determined by DISA in accordance with DoDD 4640.13 and DoDI 4640.14, unless you are waived from this guidance or are not a DoD customer.

? **(M)**-Mandatory items must be completed prior to the request being submitted.

-This help link takes you to the description within DISAC310-130-5.

**Figure 2: Type of Service Page**

**ACTION:** ARO/APO selects “Establish a VPN” for the request action under “Virtual Private Networks (VPNs)” as shown below.

Note: This action type is NOT available for Private Data ISP Service, IAP DMZ, CMNT COI (now Layer 3 only), and MPG/NFG COI VPN type services. See sections 6.6, 6.7, 6.8, and 6.9.

**Request Action Page**

[DISA Direct Home](#)   [New Notifications](#)   [TR Home](#)   [TR Help](#)   [Track TR](#)   [CAD](#)   [ABD](#)

(M) Select a type action:

**Virtual Private Networks (VPNs)**

- Establish a VPN
- Change VPN Point of Contact (POC) Information
- Discontinue a VPN (**Prerequisite Info:** All VPN connections must be disconnected first.)

**VPN Connections**

- Connect to a VPN (**Prerequisite Info:** VPN must be established.)
- Amend a VPN Connection
- Change VPN Connection Information
- Cancel a VPN Connection
- Discontinue a VPN Connection

---

(M)-Mandatory items must be completed prior to the request being submitted.

-This help link takes you to the description within DISAC310-130-5.

**Figure 3: Request Action Page**

**ACTION:** ARO/APO completes the General Information Page as shown below, and clicks “Continue.”

**General Information**

[DISA Direct Home](#)   [Notifications](#)   [TR Home](#)   [TR Help](#)   [Track TR](#)   [CAD](#)   [ABD](#)

**WARNING!** Use of the Back and Forward buttons on the browser may cause undesired results, therefore they should NOT be used to navigate through the request.

? (M) Document Classification: UNCLAS

### General Information

? (M) This requirement is for **DISN Virtual Private Network (VPN)**

? (M) Geographical Disposition

Select the areas representing the service points that will be included in this request:

CONUS (Areas 1,2)  EUR (Areas 3,4,5,6)  PAC (Areas 7,8,9)

### Product & Service Requirements

? (M) Product/Service Description:

Establish a VPN

### Related Request Numbers

? Customer Job Order Number (CJON)/Tracking Number:

Number of CJONs to add:

### VPN TR Routing Information

? (M) VPN Routing ID: DISA01 - DISA01 - DISA VPN MATRIX 1

Note: The VPN Routing ID is a six-position number assigned by your Agency's [Routing List Official](#).

**VPN Routing ID List - DISA01**  
DISA01 - DISA VPN MATRIX  
1

Members

Seq	Type	Member	Agency	Org
1	Office	DISA VPN Office 1		
	<a href="#">BADGETT</a>	Badgett, Sheila	Defense Information Systems Agency (DISA)	Network Services Directorate - NS
	<a href="#">HENRY</a>	Henry, John	Defense Information Systems Agency (DISA)	Network Services Directorate - NS
	<a href="#">LAKEINM</a>	Lakeinm, Vince	Defense Information Systems Agency (DISA)	DISA CONUS
	<a href="#">LAKE</a>	Lake, Vince	Defense Information Systems Agency (DISA)	Network Services Directorate - NS

Figure 4: General Information Page

**General Information Page – VPN Details:**

1. **General Information** – this section automatically displays the type service name [e.g., DISN Virtual Private Network (VPN)].
  - a. **Geographical Disposition** – mandatory selection to indicate the area. Select one or more of the areas that represent the VPN location.
2. **Product & Service Requirements** – this mandatory text field will automatically populate with the type action selected: Establish a VPN. Additional product/service description information may be added.
3. **Related Request Numbers** – this section is optional on all TRs and allows additional Customer Job Order Numbers (CJONs) to be added to track the requirement.
4. **VPN TR Routing Information** – Establishing a VPN does not require funding using the Program Designator Code (PDC). However, in order to coordinate the service request, a VPN Routing ID is used. The Agency Routing List Official (RLO) is responsible for setting up and maintaining VPN Routing IDs. All VPN routing IDs that the RLO has set up will automatically be presented in the VPN Routing Information section. If no VPN Routing IDs are shown or a new VPN Routing ID is required, the RLO hyperlink should be selected in order to contract your agency’s RLO. Note: customers must fund for any access circuit to a non-DSS subscription site if it is required.
  - a. **VPN Routing ID** – mandatory selection.

**ACTION:** ARO/APO completes the Virtual Private Network (VPN) Information Page as shown below, selecting the type of VPN, either L2, L3, TE, or CX, and clicks “Continue.”

**Establish a VPN Information Page**

DISA Direct Home   Notifications   TR Home   TR Help   Track TR   CAD   ABD

## DISN Virtual Private Network (VPN) - Establish a VPN - Start

**CJON: WO20AUG124664**

■ =Current Page  
■ =Optional  
■ =Mandatory Data Complete  
■ =Mandatory Data Incomplete

CCO/CMOM E N U

**Requester Info**

**VPN Details**

**VPN Info**

**Summary**

(M) = Mandatory  
(R) = Recommended

Recommended  
DISAC 310-130-5  
Matrix

? = Help

**WARNING! Use of the Back and Forward buttons on the browser may cause undesired results, therefore they should NOT be used to navigate through the request.**

**Virtual Private Network (VPN) Information**

? VPN ID:  *Note: VPN ID is generated upon final routing approval of the Telecom Request (TR)*

? (M) Select the Agency requiring the VPN service:

*If your Agency is not listed please contact the [REQUESTFULFILLMENTPROCESSMGMT@DISA.MIL](mailto:REQUESTFULFILLMENTPROCESSMGMT@DISA.MIL) or [RFMP@DISA.MIL](mailto:RFMP@DISA.MIL)*

? (M) Type of VPN:

Select from the following type in the table below:

L3	Private IP Service (Layer 3 VPN)
L2	Private LAN Service (Layer 2 VPN)
CX	Label Transport Service (Layer 2 CsC)
TE	DISN Test & Evaluation Service (DTES – Layer 3 VPN)

Figure 5: Establish a VPN Information Page

**Establish a VPN Information Page:**

1. **Virtual Private Network (VPN) Information** – this section provides the VPN ID, the Agency requiring the service, and the type of VPN.
  - a. **VPN ID** – this is a display field. The VPN ID is generated upon final routing approval of the Telecommunications Request (TR).

- b. **Select the Agency requiring the VPN service** –select the agency that requires the VPN service. This is a mandatory selection. The Agency code and description are based upon the DISAC 310-65-1 Chapter 3 “Agency Requiring the Service,” Para C3.4 “Listing of Codes.” If the agency is not listed, select the content e-mail provided (hyperlinked e-mail address on the page) to send an email to request the agency name to be added.
- c. **Type of VPN** – the type of VPN service is available in the drop down menu for either L2, L3, CX, or TE. The examples provided below are the “L3 - Private IP Service (Layer 3 VPN)” type of VPN.

**2. VPN Point of Contact Information.**

- a. **Primary POC** – a selection of a Primary POC is mandated in order to identify a POC at the VPN location. The POC selection information is accessed by selecting the ‘Retrieve/Enter POC Information’ or ‘Retrieve/Enter Special POC Information’. The user retrieves the mandatory Primary POC information by searching the Central Address Directory (CAD).
- b. **Alternate POC** – an additional POC at the VPN site is highly recommended in case the Primary POC is not available. The POC selection information is accessed by selecting the ‘Retrieve/Enter POC Information’ or ‘Retrieve/Enter Special POC Information’.

**ACTION:** ARO/APO continues to the Summary Page. The Summary Page reflects all of the TR information. The user has the option to “Delete Draft,” “Save as Draft,” or “Submit Request.” The following example is of a submitted request.

<b>Top Half of Summary Page</b>	
CJON: WO13APR121834	
<b>DISN Virtual Private Network (VPN) - Establish a VPN - Start</b>	
Requester Information	
<b>Rank/Title:</b>	Ms
<b>Last, First MI:</b>	Turner, Betsy L - Contractor
<b>Agency:</b>	Defense Information Systems Agency (DISA)
<b>Organization:</b>	Network Services Directorate - NS
<b>UNCLAS User E-mail:</b>	email address
<b>CLASSIFIED User E-mail:</b>	
<b>Cmcl. Phone:</b>	phone number
<b>UNCLAS Org E-mail:</b>	
<b>CLASSIFIED Org E-mail:</b>	
<b>DSN Phone:</b>	
<b>DISN Virtual Private Network (VPN) Details</b>	
General Information	

<b>Document Classification:</b>	UNCLAS
<b>Type of Service:</b>	DISN Virtual Private Network (VPN) - L3 - Private IP Service (Layer 3 VPN)
<b>Geographical Disposition:</b>	CONUS
Product & Service Requirements	
<b>Product/Service Description:</b>	Establish a VPN
Related Request Numbers	
<b>CJON(s)/Tracking Number(s):</b>	WO13APR121834
VPN TR Routing Information	
<b>VPN Routing ID:</b>	DISA01 - DISA01 - DISA VPN MATRIX 1

Figure 6: Example of Submitted Request Summary Page – Top Half

Bottom Half of Summary Page			
DISN Virtual Private Network (VPN) Information			
<b>VPN ID:</b>			
<b>Agency Requiring VPN:</b>		DK - Defense Information Systems Agency - Department of Defense	
<b>Type of VPN:</b>		L3 - Private IP Service (Layer 3 VPN)	
Primary VPN POC			
<b>Name:</b>	<b>UNCLAS User E-mail:</b>	<b>UNCLAS Org E-mail:</b>	
<b>CLASSIFIED User E-mail:</b>	<b>CLASSIFIED Org E-mail:</b>		
<b>Cmcl. Phone:</b>	<b>DSN Phone:</b>	<b>Pager:</b>	
Alternate VPN POC			
<b>Name:</b>	<b>UNCLAS User E-mail:</b>	<b>UNCLAS Org E-mail:</b>	
<b>CLASSIFIED User E-mail:</b>	<b>CLASSIFIED Org E-mail:</b>		
<b>Cmcl. Phone:</b>	<b>DSN Phone:</b>	<b>Pager:</b>	
<p>The following list contains the E-mail addresses of the activities that will receive an electronic copy of this request once the final approval has been completed. You may add addressees to this list. You may also use CAD to retrieve E-mail addresses.</p>			
E-mail Addresses			
<b>TO:</b>			
DISACONTESTIPCMO@disa.mil			
<b>CC:</b>			
UNCLAS E-mail		UNCLAS E-mail	
Approval Routing List			

Sequence	Approver / Office	Status	Comments
1	<a href="#">DISA VPN Office</a>	Pending (notified 13 Apr 2012 08:42:15)	

Figure 7: Example of Submitted Request Summary Page – Bottom Half

**Summary Page:**

1. The user has three options on the Summary Page:
  - a. **Delete Draft** – allows the user to delete the requirement from the database.
  - b. **Save as Draft** – allows the user to save the information and return to complete later.
  - c. **Submit Request** – automatically changes the status of the TR to “Pending” and notifies the first routee in the VPN Routing List.
  
2. Upon final approval in the routing, an e-mail will be generated and sent to the engineering e-mail addresses based upon the geographical disposition indicated in the TR. In addition, all POCs and any additional e-mail addresses added on the TR will be included on the e-mail.

**Example of Displayed Approved Request E-mail to Establish a VPN**

[DISA Direct Home](#)   [Notifications](#)   [TR Home](#)   [TR Help](#)   [Track TR](#)   [CAD](#)   [ABD](#)

**CJON: WO13APR121834**

From: cmwebtest@disa.mil  
 To: DISACONTESTIPCMO@DISA.MIL  
 Cc: SHEILA.BADGETT@DISA.MIL, BETSY.TURNER.CTR@DISA.MIL  
 Subject: DISN Virtual Private Network (VPN) -  
 Layer 3 VPN (Private Internet Protocol (IP) Service) -  
 CJON: WO13APR121834 VPN ID: DKL300201

The subject DISA Direct Telecom Request (TR) to establish a VPN has been approved.

Connection to this VPN ID is requested by creating and submitting a DISA Direct Telecom Request (TR).

Select "DISN Virtual Private Network (VPN)" as the type service. Select the "Connect to a VPN" request action.

Complete the TR and submit!

If questions, please contact the DISN Global Support Center (DGSC) at  
 CONUS ONLY (800) 554-3476 Option 2  
 CMCL (614) 692-4790 Option 2  
 DSN (510) 376-3472 or (312) 850-4790 Option 2

[DISA.DGSC@MAIL.MIL](mailto:DISA.DGSC@MAIL.MIL)  
Global DSN: (510) 376-3222  
Thank you.

Figure 8: Example of Auto-Generated E-mail of Approved Request to Establish a VPN

**Other Informational Notes:**

**TR Homepage Options**

1. **Copy Existing TR** – does not apply to “Establish a VPN”; will only apply to “Connect to an Established VPN.”
2. **Import a TSR** – does not apply to any of the VPN services.
3. **Retrieve a Draft TR** – applies to both “Establish a VPN” and “Connect to an Established VPN.”
4. **Review Submitted TR** – applies to both “Establish a VPN” and “Connect to an Established VPN.”
5. **Recall a TR** – applies to both “Establish a VPN” and “Connect to an Established VPN.”
6. **Track TR** – applies to both “Establish a VPN” and “Connect to an Established VPN.”

## 10. Other Action Requests – VPNs

Once the “Establish a VPN” has been submitted, the “Change VPN Point of Contact (POC) Information” option may be used to change the Primary or Alternate POC information. When the request is submitted, it will route based upon the VPN Routing ID identified on the TR. Upon final approval of the TR, an e-mail will be generated and sent to all e-mail addresses indicated on the TR Summary page. The “Discontinue a VPN” option is used to discontinue the use of the overall VPN. Before this action is taken, all of the VPN connections must be discontinued with the actions all completed. The “VPN Connections” section actions are addressed in the *Connect to an Established VPN* Customer Ordering Guide.

(M) Select a type action:

### Virtual Private Networks (VPNs)

- Establish a VPN
- Change VPN Point of Contact (POC) Information
- Discontinue a VPN (**Prerequisite Info:** All VPN connections must be disconnected first.)

### VPN Connections

- Connect to a VPN (**Prerequisite Info:** VPN must be established.)
- Amend a VPN Connection
- Change VPN Connection Information
- Cancel a VPN Connection
- Discontinue a VPN Connection

---

 (M)-Mandatory items must be completed prior to the request being submitted.

 -This help link takes you to the description within DISAC310-130-5.

**Figure 9: Request Action Page for Other Actions**

## Appendix A Acronym List

Acronym	Term
APO	Authorized Provisioning Official
AR	Aggregation Router
ARO	Authorized Requesting Official
ATM	Asynchronous Transfer Mode
CAD	Central Address Directory
CAP	Connection Approval Process
CCSD	Command Communications Service Designator
CENTRIXS	Combined Enterprise Regional Information Exchange System
CJON	Customer Job Order Number
CMNT	Common Mission Network Transport
CNDSP	Computer Network Defense Service Provider
COI	Community of Interest
COMSEC	Communications Security
CsC	Carrier supporting Carrier
DCN	DISA Control Number
DDOE	DISA Direct Order Entry
DECC	Defense Enterprise Computing Center
DGSC	DISN Global Support Center
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DMZ	Demilitarized Zone
DoD	Department of Defense
DSS	DISN Subscription Service

Acronym	Term
DTES	DISN Test & Evaluation Service
DWCF	Defense Working Capital Fund
eBGP	External Border Gateway Protocol
FY	Fiscal Year
GIAP	GIG Interconnection Approval Process
GIG	Global Information Grid
GNSC	Global NetOps Support Center
IA	Information Assurance
IAP	Internet Access Point
ID	Identifier
iEHR	integrated Electronic Health Records
IP	Internet Protocol
IPT-PE	IP Transport Provider Edge
ISP	Internet Service Provider
LAN	Local Area Network
MPLS	Multiprotocol Label Switching
LSTDM	Low-Speed Time Division Multiplexing
Med COI	Medical Community of Interest
MPG	Mission Partner Gateway
NFE	NIPRNet Federated Gateway External
NFG	NIPRNet Federated Gateway
NFI	MPG/NFG Internal
NIPRNet	Unclassified but Sensitive IP Router Network
NS	Network Services Directorate
PDC	Program Designator Code
POC	Point of Contact
RLO	Routing List Official

Acronym	Term
SBU	Sensitive but Unclassified
SGS	SIPRNet GIAP System
SIPRNet	Secret IP Router Network
SLA	Service Level Agreement
SNAP	System/Network Approval Process
TR	Telecommunications Request
TSR	Telecommunications Service Request
UPE	Unclassified Provider Edge
VA	Department of Veterans Affairs
VPN	Virtual Private Network



Defense Information Systems Agency  
P.O. Box 549  
Ft. Meade, MD 20755-0549  
[www.disa.mil](http://www.disa.mil)