



Defense Information Systems Agency

**A Combat Support Agency**

# **NETWORK SERVICES**

## **VIRTUAL PRIVATE NETWORKS**

### **CONNECT TO AN ESTABLISHED VIRTUAL PRIVATE NETWORK (VPN) CUSTOMER ORDERING GUIDE**

Version 2.5  
May 13, 2013

**UNCLASSIFIED**

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

This page intentionally left blank.

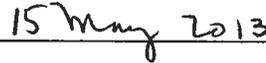
## Signature Page for Key Officials

*Approved by:*



MARTHA.O.BUCK

Chief, Customer Services Division (NSP4)



Date

This page intentionally left blank.



<b>1. Introduction.....</b>	<b>1</b>
<b>2. Purpose.....</b>	<b>2</b>
<b>3. References.....</b>	<b>2</b>
<b>4. Roles and Responsibilities .....</b>	<b>2</b>
<b>5. Points of Contact .....</b>	<b>2</b>
<b>6. VPN Services Descriptions .....</b>	<b>3</b>
6.1 Private IP Service (Layer 3 VPN).....	3
6.2 Private LAN Service (Layer 2 VPN) .....	3
6.3 Label Transport Service (Layer 2 VPN).....	3
6.4 DISN Test and Evaluation Network (DTEN – Layer 3 VPN).....	4
6.5 Secret Private IP Service (Classified Layer 3 VPN).....	4
6.6 Private ISP Service (Layer 3 VPN) .....	4
6.7 IAP Gateway at DECC (Layer 3 VPN) .....	4
6.8 NIPRNet Federated Gateway (NFG) Community of Interest (COI) (Layer 3 VPN).....	5
6.9 CMNT COI (Layer 3 VPN).....	6
6.10 Med COI Service (Layer 3 VPN) .....	6
<b>7. Process Overview .....</b>	<b>7</b>
<b>8. Business Rules .....</b>	<b>9</b>
<b>9. Steps to Connect to an Established VPN on DDOE .....</b>	<b>10</b>
<b>10. Other Action Requests – VPN Connections .....</b>	<b>28</b>
<b>Appendix A Acronym List.....</b>	<b>29</b>

## List of Illustrations

<b>Table 1: VPN Services .....</b>	<b>1</b>
<b>Table 2: Points of Contact.....</b>	<b>2</b>
<b>Figure 1: Process to Connect to an Establish VPN.....</b>	<b>8</b>
<b>Figure 2: Type of Service Page .....</b>	<b>11</b>
<b>Figure 3: Request Action Page.....</b>	<b>11</b>
<b>Figure 4: Example of Search Page .....</b>	<b>12</b>
<b>Figure 5: General Information Page.....</b>	<b>14</b>
<b>Figure 6: Product &amp; Service Requirements Page .....</b>	<b>16</b>
<b>Figure 7: Connect to a VPN Information Page.....</b>	<b>18</b>
<b>Figure 8: Example of TR to Connect to a VPN Summary Page.....</b>	<b>24</b>
<b>Figure 9: Example of TSR to Connect to an Established L3 VPN.....</b>	<b>26</b>
<b>Figure 10: Request Action Page for Other Actions .....</b>	<b>28</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. 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 **Establish a VPN** and the second step **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> or <https://snap.dod.mil>. In addition, the appendices of the Connection Process Guide (CPG) 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) or <https://giap.disa.smil.mil>.

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 Network (DTEN – Layer 3 VPN)
DKL300251	Medical Community of Interest (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>
C3	<b>FUTURE</b> – SIPRNet Private IP Service (Classified Layer 3 VPN)
DKL300227	<b>FUTURE</b> – Private ISP Service (All Customers – Layer 3 VPN) - <i>Customers can ONLY submit "Connect to an established VPN" requests for this service</i>
DOL300230	<b>FUTURE</b> – IAP Gateway at DECC (All Customers – Layer 3 VPN) - <i>Customers can ONLY submit "Connect to an established VPN" requests for this service</i>
DKL300249	<b>FUTURE</b> – 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.**

The L3 Private IP Service (Layer 3 VPN), the L2 Private Local Area Network (LAN) Service (Layer 2 VPN), CX Label Transport Service (Layer 2 CsC VPN), TE DISN Test & Evaluation

Network (DTEN – Layer 3 VPN), Common Mission Network Transport (CMNT) Community of Interest (CMNT COI – Layer 3 VPN), and Medical Community of Interest (Med COI – Layer 3 VPN) are available now for ordering via DISA Direct Order Entry (DDOE). The other VPN services will be available within the next Fiscal Year (FY) 2014. A notice 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 *Connect to an Established VPN* via DISA Direct Order Entry (DDOE) for Private IP Service (Layer 3 VPN), Private LAN Service (Layer 2 VPN), Label Transport Service (Layer 2 CsC VPN), and DISN Test & Evaluation Network (DTEN – Layer 3 VPN). It includes minor differences in ordering associated with Private ISP Service, IAP Gateway at DECC, Common Mission Network Transport (CMNT) Community of Interest (COI) (now Layer 3 only), Medical Community of Interest (Med COI – Layer 3 VPN), and NIPRNet Federated Gateway (NFG) Community of Interest (COI) VPN services. New functionality in DDOE has also been added to allow users to change an existing connection to an established VPN Identifier (ID), to a different VPN ID. A separate Ordering Guide has been developed to address information to *Establish a 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 4.1, dated September 2012

## 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 DISN VPNs, contact the DISN Global Support Center (DGSC) using the information provided below.

DISN Global Support Center (DGSC)	
Customer Services Division (NSP4)	CML: (800) 554-DISN (3476) or (614) 692-4790 DSN: (312) 850-4790 Global DSN: (510) 376-3222 Unclassified e-mail: <a href="mailto:DGSC@csd.disa.mil">DGSC@csd.disa.mil</a> Classified 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 at any DSS location that includes Unclassified but Sensitive IP Router Network (NIPRNet) IP Data. 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 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 Network (DTEN – Layer 3 VPN)**

Test and Evaluation (T&E) IP data (operating over the DTEN) is a DISN Subscription Service (DSS rates in effect). This VPN service provides a BLACK transport capability riding the DISN Backbone. It offers standard DISN services and Service Level Agreements (SLAs) to DTEN customers. It includes provisioning and network operations support by Global NetOps Support Center (GNSC) to DTEN customers [part of Network Services Directorate (NS) Defense Working Capital Fund (DWCF)], as well as network defense through Computer Network Defense Service Provider (CNDSP) services to all DISN/DTEN customers. In addition, this service includes key management and maintenance of DISN/DTEN encryption devices.

## **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 Router Network (SIPRNet). This service is available as part of the DSS at any DSS location that includes SIPRNet IP Data. 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 ISP Service (Layer 3 VPN)**

This VPN service provides customers the ability to obtain internet access through an MPLS layer 3 VPN at any DISN Internet Access Point (IAP) as part of the DSS bandwidth. Private 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 at any DSS location that includes NIPRNet IP Data. 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*.

## **6.7 IAP Gateway at DECC (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 as part of the DSS bandwidth. It is an enterprise VPN service providing IAP internet access to customers across the DISN. This service is available as part of the DSS at any DSS location that includes NIPRNet IP Data.

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 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 NIPRNet. This introduces a potential threat to the NIPRNet 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 NIPRNet Federated Gateways (NFG) at multiple IAP locations to provide a secure and robust means for these agencies to connect to the NIPRNet. The benefit is that it will provide protection from and visibility into threats and events involving traffic to/from these agencies and partners. NFG shall support customers using physical/logical connections (described below as “External Customer Connecting Directly to NFE Router” and “External Customer on NIPRNet”). The system shall support logical traffic separation as traffic transits through NIPRNet.

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

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 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 NIPRNet.** The second type is a mission partner currently connecting directly to NIPRNet. This type of customer sometimes has their own back-end connection to the Internet. The goal of this NFG design is to leverage the existing connections to NIPRNet 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 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 NIPRNet to sense traffic before the NFE and IA components inspect it. The NFE routers from all 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 NFG Community of Interest (COI). The VPN ID for the 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*.

## **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 SIPRNet, thereby eliminating CENTRIXS’ dependence upon SIPRNet 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 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, NIPRNet, or SIPRNet. 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)**

The Medical Community of Interest (Med COI) service 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 at any DSS location that includes NIPRNet IP Data. 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 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 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 (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.

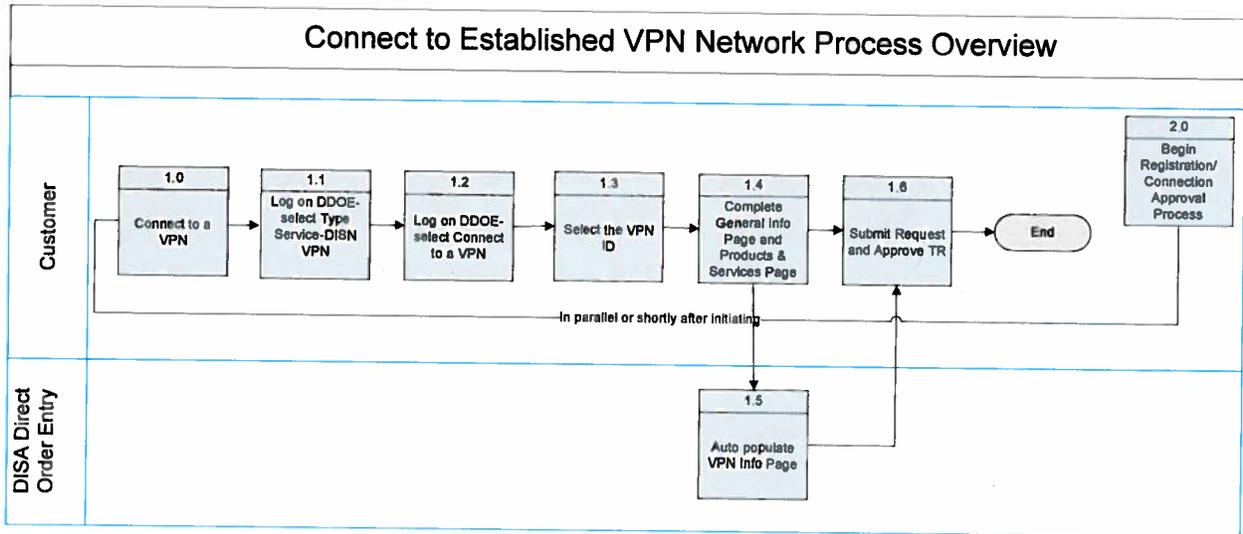
## **7. Process Overview**

The process to connect to a VPN is required for each location participating in the VPN. It is similar to the existing process for ordering connections to the SBU IP Data service (formerly known as NIPRNet). This service option will result in a Telecommunications Service Request (TSR) being generated (for each individual customer connection to the VPN) and sent to the applicable DISA Provisioning Center. The basic procedures are:

1. The authorized DDOE user may order connections only to VPNs established by his or her organization. VPN connections may be ordered on behalf of another organization, if the originating organization desires their participation.
2. The authorized DDOE user logs into DDOE and selects type of service [i.e., DISN Virtual Private Network (VPN)] and “Connect to a VPN.”
3. The authorized DDOE user will see only the VPNs established by his or her organization, and will select from that list.
4. The remaining steps follow existing DDOE NIPRNet ordering procedures.

- In parallel, or shortly after initiating the request to connect to a VPN through DDOE, the customer should begin the Registration/Connection Approval Process as outlined in Appendix M of the Connection Process Guide (GPC).

The following depicts the process overview for creating requests for individual customer connections to an established VPN. Business rules and specific steps are documented in subsequent sections.



**Figure 1: Process to Connect to an Establish VPN**

## 8. Business Rules

Ordering of the DISN VPNs is based on the basic premise and template for ordering the SBU IP Data service. Additional business rules apply when ordering this service.

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 *Connect to an Established VPN* are: Connect to a VPN, Amend, Change, Cancel, or Discontinue a VPN connection. These actions are performed on the individual physical connections to the established VPN. The following rules apply when performing actions for a VPN connection:
  - a. All “Connect to a VPN” actions will be in accordance with the Telecommunications Request (TR)/TSR process. The NIPRNet TR pages are the baseline used for the technical specifications for all of the “Connect to a VPN” type actions.
  - b. No funding is required as this service falls within the DISN Subscription Services (DSS). However, the service will also be accessible from non-DSS sites; therefore, the customer will be responsible for access circuit costs from non-DSS sites.
  - c. Program Designator Code (PDC) funding is mandated for all actions related to the connection, regardless if there is funding associated with the requirement or not.
  - d. VPN Routing IDs must have been established by the Agency Routing List Official (RLO) along with the VPN routing matrix, or a PDC routing matrix. These are available for selection when creating the TR. Additionally, a drop down menu of RLOs is available if unknown.
3. Functionality in DDOE has also been added to allow users to change an existing connection to an established VPN ID, to a different VPN ID. For “*inter-agency*” VPN ID changes, if the user requires re-connecting to the original VPN ID, a new request will need to be submitted and will require approval by the owner-agency.
4. Med COI users must use the DISA Control Number (DCN) code for this service which is D314.

## 9. Steps to Connect to an Established VPN on DDOE

This section provides steps necessary to request individual physical VPN connections to an established VPN (network). *The VPN must be established prior to requesting physical connections.* Private ISP Service, IAP Gateway at DECC, CMNT COI, Med COI, and NFG COI are DISA NS established VPNs. Customers can not 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.

All the steps and screens for connecting to an established VPN are the same for all the VPN service types (L2, L3, CX, and TE). The examples provided are specifically for the L3 - Private IP Service (Layer 3 VPN).

**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**

[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 “Connect to a VPN” for the request action under “VPN Connections” as shown below.

**Request Action Page**

[DISA Direct Home](#)   [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:** The search page presented will vary depending upon the role of the user logged into DDOE. It will also include all the VPN IDs of established VPNs created for the user. The user selects the applicable VPN ID from the pull down menu screen for the established L2, L3, TE, or CX VPN service types. The VPN ID will have been auto-generated and provided to the user in the approval email for the Establish a VPN TR.

**Example of Search Page if ARO Role**

**(NOTE: The VPN ID assignment/selection is auto-generated based on selection of Agency established VPN)**

**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)** Select the Agency that the VPN was established for:

?

**(M)** Select the Virtual Private Network (VPN) ID:

? VPN ID:

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

**Figure 4: Example of Search Page**

VPN ID information shown will consist of the VPN ID and the Geographical Disposition information (e.g., AAL300214 – CONUS/EUROPE/PACIFIC, AAL300215 – PACIFIC).

**ACTION:** The search result presents the General Information page for the user to begin completing the connection request.

### General Information Page

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

## DISN Virtual Private Network (VPN) - Connect to a VPN - Start

**CJON: WO02MAY124300 TCO Code: WO**

**?** MENU

- Requester Info
- General Info
- Product/Service Remts
- VPN Info
- Technical Info
- Dual Homing
- Diversity & Avoidance
- Funding Info
- DISA Cost Criteria
- Identification Info
- Related Requests
- Justification/Approval
- Service Point 1
- Summary

(M) = Mandatory  
(R) = 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.

**?** (M) Document Classification:

### General Information

**?** (M) This requirement **DISN Virtual Private Network (VPN)** is for **- Private IP Service (Layer 3 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](#))

**?** Select Agency ONLY if request is being submitted on behalf of an Agency and/or Organization other than your own:

---

**?** (M) Select Organization Account:

---

DA - DISA (Misc DISA HQ requirements not reflected elsew here in this table)

### Telecommunication Service Priority (TSP) Information

Select all that apply:

**?** Provisioning Priority    **?** Restoration Priority

? Provide previously authorized TSP Number: TSP

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

? (R)-Recommended items should be completed whenever possible to avoid delays in processing your requirement.

[DISAC 310-130-5 Matrix](#)-Identifies the items utilized for this type of request

? -This help link takes you to the description within DISAC 310-130-5.

Figure 5: General Information Page

**General Information Page:**

1. **General Information** – this section automatically displays the type service name based on the VPN ID selected [e.g., DISN Virtual Private Network (VPN) – Private IP Service (Layer 3 VPN)]. There are currently five exceptions. When connecting to Private ISP Service, VPN Identifier: *DKL300227*, IAP Gateway at DECC, VPN Identifier: *DOL300230*, CMNT COI Layer 3, VPN Identifier: *DKL342000*, Med COI Layer 3, VPN Identifier: *DKL300251*, and NFG COI, VPN Identifier: *DKL300249*, the Private IP Service (Layer 3 VPN) will be displayed.
  - a. **Geographical Disposition** – mandatory selection to indicate the area the service points will represent.
  - b. **Select Agency ONLY if request is being submitted on behalf of an Agency and/or Organization other than your own** – this optional selection allows the ARO/APO to indicate if the connection is being written on behalf of another agency.
  - c. **Select Organization Account** – mandatory selection that is presented when applicable for the Telecommunications Certification Office (TCO) code.
2. **Telecommunication Service Priority (TSP) Information** – this section is optional and must be completed if TSP is required.

**ACTION:** Product & Service Requirements page is presented as shown below. The Product/Service Description is auto-populated with "Connect to a VPN."

Product & Service Requirements Page

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

## DISN Virtual Private Network (VPN) - Connect to a VPN - Start

**CJON: WO02MAY124300 TCO Code: DA**

**?** MENU

- Requester Info
- General Info
- Product/Service Rqmts
- VPN Info
- Technical Info
- Dual Homing
- Diversity & Avoidance
- Funding Info
- DISA Cost Criteria
- Identification Info
- Related Requests
- Justification/Approval
- Service Point 1
- Summary**

(M) = Mandatory  
(R) = 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.

Product & Service Requirements

**?** (M) Product/Service Description:

Connect to a VPN

**?** (M) Operational Service Date:

6 Jul 2012  
(DD MMM YYYY)

Lead Time Table(s)

**?** After The Fact (ATF) or Sooner If Possible (SIP)   [CONUS](#)

**?** Requested CMCL/GFE Service Date:

6 Jul 2012  
(DD MMM YYYY)

**?** After The Fact (ATF) or Sooner If Possible (SIP)

**?** (M) Estimated Service Life:

120 (In Months, not to exceed 120)

The screenshot shows a web form with a 'Remarks' field. The field contains the text 'Connect to established VPN network'. Below the field, there are four help items, each starting with a question mark icon: 1. '(M)-Mandatory items must be completed prior to the request being submitted.' 2. '(R)-Recommended items should be completed whenever possible to avoid delays in processing your requirement.' 3. '[DISAC 310-130-5 Matrix](#)-Identifies the items utilized for this type of request' 4. '-This help link takes you to the description within DISAC 310-130-5.'

Figure 6: Product & Service Requirements Page

**Product & Service Requirements Page:**

1. **Product/Service Requirements** – this section lists the specified requirements for the connection.
  - a. **Product/Service Description** – this mandatory text field will automatically populate with the type action selected: Connect to a VPN.” This is the option the ARO/APO selected. The user may modify or insert additional information.
  - b. **Operational Service Date** – mandatory field for the operational service date.
  - c. **Requested CMCL/GFE Service Date** – mandatory field for the requested service date.
  - d. **Estimated Service Life** – this is a recommended field to indicate the length of time for the connection.
  - e. **Remarks** – this is an optional field for any remarks information.

**ACTION:** Virtual Private Network (VPN) Information page is presented as shown below. The page is auto-populated with the VPN Information such as VPN ID, Agency Requiring the VPN, Type of VPN (L2, L3, CX, or TE), and the VPN POCs that were indicated on the Establish a VPN request.

**Connect to a VPN Information Page**

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

## DISN Virtual Private Network (VPN) - Connect to a VPN

**CJON: WO13APR121836   TCO Code: DA**

**?** **MENU**

- Requester Info
- General Info
- Product/Service Rqmts
- VPN Info
- Technical Info
- Dual Homing
- Diversity & Avoidance
- Funding Info
- Identification Info
- Related Requests
- Justification/Approval
- Service Point 1
- Service Point Mgmt
- Summary

**(M)** = Mandatory  
**(R)** = 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: **DKL300201**   *Note: VPN ID is generated upon final routing approval of the Telecom Request (TR)*

**?** **(M)** Select the Agency requiring the VPN service: **DK - Defense Information Systems Agency - Department of Defense**

**?** **(M)** Type of VPN: **L3 - Private IP Service (Layer 3 VPN)**

**VPN Point of Contact Information**

**?** **(M)** **Primary POC**

Rank/Title:	<b>Ms</b>				
Last, First MI:	<b>Turner, Betsy L - Contractor</b>				
	<a href="#">UNCLAS E-mail</a>				
User E-mail:	<a href="#">UNCLAS E-mail</a>				
Org E-mail:					
	<a href="#">CLASSIFIED E-mail</a>				
User E-mail:					
Org E-mail:					
	Intl Access	Area/Cntry	Exchange	Phone	Extension
Cmcl. Phone:		<b>301</b>	<b>555</b>	<b>1234</b>	

DSN Phone:					
Pager #:					
<b>? (R) Alternate POC</b>					
Rank/Title:	<b>Ms</b>				
Last, First MI:	<b>Badgett, Sheila - Government</b>				
	<a href="#">UNCLAS E-mail</a>				
User E-mail:					
Org E-mail:	<a href="#">UNCLAS E-mail</a>				
	<a href="#">CLASSIFIED E-mail</a>				
User E-mail:					
Org E-mail:					
	Intl Access	Area/Cntry	Exchange	Phone	Extension
Cmcl. Phone:		<b>618</b>	<b>555</b>	<b>1234</b>	
DSN Phone:					
Pager #:					

**VPN TR Routing Information**

**? (M) VPN Routing ID:**

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="#">LAKEIN</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 7: Connect to a VPN Information Page

**Connect to 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 (L2, L3, TE, or CX).
  - a. **VPN ID** – displays the full VPN ID that was selected on the SEARCH page.
  - b. **Select the Agency requiring the VPN service** – displays the first and second position code of the VPN ID along with the description based upon DISAC 310-65-1 Chapter 3 “Agency Requiring the Service,” Para C3.4 “Listing of Codes” (e.g., AA – Office of Secretary of Agriculture – Department of Agriculture).
  - c. **Type of VPN** – the type of VPN service will automatically be displayed L2, L3, CX, or TE. There are currently five exceptions. When connecting to Private ISP Service, VPN Identifier: *DKL300227*, IAP Gateway at DECC, VPN Identifier: *DOL300230*, CMNT COI Layer 3, VPN Identifier: *DKL342000*, Med COI Layer 3, VPN Identifier: *DKL300251*, and NFG COI, VPN Identifier: *DKL300249*, the L3 - Private IP Service (Layer 3 VPN) will be displayed. The example is for a “L3 - Private IP Service (Layer 3 VPN).”
2. **VPN Point of Contact Information** – this section provides the primary and alternate POC information for the VPN.
3. **VPN TR Routing Information** – the **VPN Routing ID** is a mandatory selection. It will auto-populate with the VPN Routing ID that was used on the “Establish a VPN” TR. This routing is in addition to the PDC routing. The five exceptions are Private ISP Service, IAP Gateway at DECC, CMNT COI (now Layer 3 only), Med COI Layer 3, and NFG COI VPN types. For Private ISP Service select VPN Identifier: *DKL300227*. For CMNT COI Layer 3 select VPN Identifier: *DKL342000*. For NFG COI select VPN Identifier: *DKL300249*. For Med COI Layer 3 select VPN identifier: *DKL300251*. See sections 6.6, 6.7, 6.8, 6.9, and 6.10.

**Complete the remaining request items as when ordering SBU IP Data service (formerly known as NIPRNet).**

**Identification Information Page:**

Complete information for your Command Communications Service Designator (CCSD).

1. **PN as the Purpose and Use Code will be automatically populated by the DDOE.** PN is for all Virtual Private Networks.
2. User must select **G** for **Permanent Virtual Circuits for entry for Type of Service.**

**ACTION:** ARO/APO continues to the Summary Page. The Summary Page reflects all of the TR information to connect to a VPN. The user must review the information. The following is a Summary Page from an example TR to connect to a VPN.

Summary Page	
<a href="#">DISA Direct Home</a> <a href="#">Notifications</a> <a href="#">TR Home</a> <a href="#">TR Help</a> <a href="#">Track TR</a> <a href="#">CAD</a> <a href="#">ABD</a>	
<p>Following is a summary of this request. You are authorized only to view this request. Click <a href="#">Return to return</a> to the TR Home page.</p> <p><b>CJON: WO02MAY124300 TCO Code: DA</b></p>	
Request Summary	
Funding Line(s)	Service Point(s)
<a href="#">1</a>	<a href="#">1</a>
DISN Virtual Private Network (VPN) - Connect to a VPN - Start	
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>	email address
<b>Cmcl. Phone:</b>	phone number
<b>UNCLAS Org E-mail:</b>	
<b>CLASSIFIED Org E-mail:</b>	
<b>DSN Phone:</b>	
General Information	
<b>Document Classification:</b>	UNCLAS
<b>Type of Service:</b>	DISN Virtual Private Network (VPN) - Private IP Service (Layer 3 VPN)
<b>Geographical Disposition:</b>	CONUS
<b>Request is being submitted on behalf of:</b>	
<b>Agency:</b>	
<b>Organization Account:</b>	DISA (Misc DISA HQ requirements not reflected elsewhere in this table)
Telecommunication Service Priority (TSP) Information	
<b>Provisioning Priority:</b>	NO
<b>Restoration Priority:</b>	NO
<b>Previously authorized TSP Number:</b>	
Product & Service Requirements	

<b>Product/Service Description:</b> Connect to a VPN		
<b>Operational Service Date:</b> 06 Jul 2012	<b>Estimated Service Life:</b> 120 months	
<b>Requested CMCL/GFE Service Date:</b> 06 Jul 2012		
<b>Remarks:</b> Connect to established VPN network		
<b>DISN Virtual Private Network (VPN) Information</b>		
<b>VPN ID:</b> DLL300212		
<b>Agency Requiring VPN:</b> DL - Defense Intelligence Agency - Department of Defense		
<b>Type of VPN:</b> L3 - Private IP Service (Layer 3 VPN)		
<b>Primary VPN POC</b>		
<b>Name:</b> Mr. Jack Buck	<b>UNCLAS User E-mail address:</b>	
<b>CLASSIFIED User E-mail:</b>	<b>UNCLAS Org E-mail:</b>	
<b>CLASSIFIED Org E-mail:</b>	<b>CLASSIFIED User E-mail:</b>	
<b>Cmcl. Phone:</b> phone	<b>DSN Phone:</b> phone	
<b>Pager:</b>		
<b>Alternate VPN POC</b>		
<b>Name:</b> Ms Betsy L Turner	<b>UNCLAS User E-mail address:</b>	
<b>CLASSIFIED User E-mail:</b>	<b>UNCLAS Org E-mail:</b>	
<b>CLASSIFIED Org E-mail:</b>	<b>CLASSIFIED User E-mail:</b>	
<b>Cmcl. Phone:</b> phone	<b>DSN Phone:</b> phone	
<b>Pager:</b>		
<b>VPN TR Routing Information</b>		
<b>VPN Routing ID:</b> DISA01 - DISA VPN MATRIX 1		
<b>Technical Information</b>		
<b>Type of Operation:</b>	Full Duplex	
<b>Do you want DISA to manage your router:</b>	NO	
<b>Modulation Rate/Bandwidth:</b>	1.544MB	
<b>Service Availability:</b>	Full Period	
<b>Signaling Mode:</b>	NO SIGNALING	
<b>Funding Information</b>		
<b>Overtime/Expedite Charges:</b>	No	
<b>Communications Service Authorization (CSA) Number:</b>	New Lease	
<b>Cost Threshold (Not to Exceed)</b>		
<b>Program Designator Code (PDC)</b>	<b>Monthly Recurring Charges (MRC)</b>	<b>Non-Recurring Charges (NRC)</b>
YMTT20	\$0.00	\$0.00
<b>DISA Cost Estimate</b>		

Cost Description	Billing Bandwidth	MRC	NRC
<b>Disclaimer</b>		The TR will be routed to a Provisioning Office for a service cost estimate.	
<p><b>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.</b></p> <p><a href="#">To DISA Cost Estimate History.</a></p>			
<b>Identification Information</b>			
<b>CCSD:</b>	<b>Agency Code:</b>	D - Defense Information Systems Agency	
	<b>Purpose/Use:</b>	PN - Private IP Service (Layer 3 VPN)	
	<b>Type of Service:</b>	G - Permanent Virtual Circuits	
	<b>Sequence ID:</b>	0001	
	<b>NSS:</b>	NO - NSS exemption not required.	
	<b>Jurisdictional Classification:</b>	100 Percent	
	<b>Is this a BRAC Requirement?</b>	NO	
	<b>DISA Control Number:</b>	Med COI users ONLY must use the DISA Control Number (DCN) code for this service which is D314.	
	<b>Exercise/Project Description:</b>	Connect to an established VPN network.	
	<b>Satellite Data Base (SDB) Approval Number:</b>		
<p>Communications Control Office/Communications Management Office (CCO/CMO) Information</p> <p><b>(CCO/CMO) Information:</b></p>			
<b>Related Request Numbers</b>			
	<b>CJON(s)/Tracking Number(s):</b>	WO02MAY124300	
	<b>Work-In-Conjunction With:</b>		
<b>Justification and Approvals</b>			
	<b>Justification of Service Requested:</b>		
	<b>Identification of Reference:</b>		
	<b>Approval Document:</b>		
	<b>Accreditation Package Information:</b>		
<b>Service Point 1: Herndon, Virginia, United States</b>			
	<b>Facility Code:</b>	1NJ-DISN NIPRNET DMZ ISOLATION ROUTER - 1ST WITHIN GEOLOC	
User Location Information			

<b>Address:</b> 1111 Test Drive HERNDON, Virginia 20171-2516			
<b>Building:</b> X	<b>Floor:</b> 1	<b>Room:</b> 101	
<b>NPA:</b> 703		<b>NXX:</b> 860	
<b>Latitude:</b>		<b>Longitude:</b>	
<b>Directions to Site:</b> Test			
Primary User POC			
<b>Name:</b> Ms Betsy L Turner - Contractor	<b>UNCLAS User E-mail:</b>	<b>email address</b>	<b>UNCLAS Org E-mail:</b>
<b>CLASSIFIED User E-mail:</b>	<b>CLASSIFIED Org E-mail:</b>		
<b>Cmcl. Phone:</b> phone	<b>DSN Phone:</b> phone	<b>Pager:</b>	
Alternate User POC			
<b>Name:</b> Ms Sheila A Badgett - Government	<b>UNCLAS User E-mail:</b>	<b>email address</b>	<b>UNCLAS Org E-mail:</b>
<b>CLASSIFIED User E-mail:</b>	<b>CLASSIFIED Org E-mail:</b>		
<b>Cmcl. Phone:</b> phone	<b>DSN Phone:</b> phone	<b>Pager:</b>	
Last Half Mile Information			
<b>Last Half Mile Site Support Declaration:</b> No			

### Service Point #1 Continued

General Service Point Information	
<b>Customer Terminal Equipment:</b> Test	
<b>Crypto Equipment:</b> UNSECURE	
Interface Specifications	
<b>Physical:</b>	RJ-41
<b>Electrical:</b>	T-1, LINE CODING: B8ZS, FRAME FORMAT: ESF
<b>Detail Interface Information:</b>	Test
<b>Unique On-site Installation Factors:</b>	Test
Inside Wire Requirements	
<b>Customer Premise Inside Wire Installation:</b>	No
<b>Customer Premise Inside Wire Maintenance:</b>	No
Security Information	
<b>Clearance Required:</b>	Yes
<b>Escort Required:</b>	Yes
<b>Security Instructions:</b>	Test

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.

E-mail Addresses			
TO:			
provtestms@disa.mil			
CC:			
		email address	
email address		DISACONTESTIPCMO@disa.mil	

Approval Routing List			
Sequence	Approver / Office	Status	Comments
1	<a href="#">DISA VPN Office</a>	Pending (notified 02 May 2012 12:52:33)	
2	<a href="#">CONUSTESTIPENG</a>		
3	<a href="#">CONUSTESTENG</a>		
4	<a href="#">DISA Default Office</a>		

Request Summary	
Funding Line(s)	Service Point(s)
<a href="#">1</a>	<a href="#">1</a>

Figure 8: Example of TR to Connect to a VPN Summary Page

**EXAMPLE:** The following is an example of a TSR for requesting a connection to an established L3 - Private IP Service (Layer 3 VPN).

```
R 141645Z AUG 12
FM ZEN NAME@MAIL.MIL
TO ZEN PROTMS@DISA.MIL
INFO ZEN NPE-MAILBOX@MAIL.MIL
ZEN NAME@MAIL.MIL
ZEN DISACONCMO@DISA.MIL
BT
UNCLAS
SUBJ: TELECOMMUNICATIONS SERVICE REQUEST
101. DA14AUG125088
103. START
104. CIRCUIT ONLY/SINGLE VENDOR
105. NIPRNET
106A. 280800Z SEP 12
106B. 280800Z SEP 12
107. DPNG0001
108. PN
110. FULL DUPLEX
111. 1.544MB
112. FULL PERIOD
115. NO SIGNALING
116. NEW LEASE
117. YXXX
118. NO
119D. NO
120A. ALBRTVLL
121A. 01
122A. C
124A. TEST; ALBERTVILLE, AL, 35951
126A. IP ROUTER
127A. UNSECURE
130A. (PMRY POC) MS SHEILA BADGETT; (CLASS USER)
NAME@MAIL.SMIL.MIL; (UNCLASS USER)
NAME@MAIL.MIL; (CMCL) 618-555-1234; (DSN) 777-1234
(ALT POC) MS BETSY L TURNER; (CLASS USER)
NAME@MAIL.SMIL.MIL; (UNCLASS USER)
NAME@MAIL.MIL; (CMCL) 571-555-4321
131A. TEST; ALBERTVILLE, AL, 35951
139A. 301/555
140A. DISA/NETWORK SERVICES DIRECTORATE - NS
401. CONNECT TO A VPN
402. DISA; NETWORK SERVICES DIRECTORATE - NS; MS BETSY TURNER;
```

(CLASS USER) NAME@MAIL.SMIL.MIL (UNCLASS USER)  
 NAME@MAIL.MIL; (CMCL) 571-555-4321  
 405. N  
 411. (SP A) CLEARANCE REQUIRED; ESCORT REQUIRED  
 413. (\*\* SHIPPING ADDR \*\*) (SP A) TEST; ALBERTVILLE, AL, 35951  
 416. (NTE MRC) \$0.00; (NTE NRC) \$0.00  
 417. \*\* ADDITIONAL INFORMATION PERTINENT TO THIS REQUIREMENT IS  
 POSTED BELOW WITH RESPECTIVE LABELS \*\*  
 (\*\*SITE SUPPORT DECLARATION AND FUNDING NUMBER INFORMATION\*\*)  
 (SP A) NO  
 (\*\* DISA COST ESTIMATE \*\*)  
 TOTAL DISA COST ESTIMATE: MRC: \$0.00; NRC: \$0.00;  
 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, SERVICE  
 POINTS (GEOLOC CODE), OR PROVISIONING CRITERIA ON ANY SERVICE POINT,  
 THEN THE TR IS REROUTED TO THE DISA ENGINEERING OFFICE.; THERE IS NO  
 COST FOR THE TYPE OF SERVICE BEING REQUESTED.;  
 (\*\* FUNDING AUTH INFO \*\*) (PDC) YXXX; (BONA FIDE NEED FY) 2012;  
 (NTE MRC) \$0.00; (NTE NRC) \$0.00; (FUNDING OFFICE) NS82 - NEW OE ROUTING  
 OFFICE; (LAFO/AFO) VINCE LAKE; NOTE: THE LINE OF ACCOUNTING (LOA) IS IN  
 TIBI FOR THE BONA FIDE NEED FISCAL YEAR.;

(\*\* GEO DISPOSITION \*\*) CONUS(AREAS 1,2)  
 (\*\* DISA MANAGED ROUTER \*\*) NO  
 (\*\* ADDITIONAL PROVISIONING INFORMATION \*\*) (ORG ACCT) DISA (MISC  
 DISA HQ REQUIREMENTS NOT REFLECTED ELSEWHERE IN THIS TABLE)  
 (\*\* BRAC REQUIREMENT \*\*) NO;  
 (\*\* VPN INFO \*\*) (AGENCY) DK - DEFENSE INFORMATION SYSTEMS AGENCY -  
 DEPARTMENT OF DEFENSE; (TYPE OF VPN) LAYER 3 VPN (PRIVATE INTERNET  
 PROTOCOL (IP) SERVICE) - L3;

(PMRY VPN POC) MS SHEILA BADGETT; (UNCLASS USER)  
 NAME@MAIL.MIL; (CMCL) 618-555-1234; (DSN)  
 777-1234; (ALT VPN POC) MS BETSY TURNER; (USER)  
 NAME@MAIL.MIL; (CMCL) 571-555-4321;  
 430. 120 MONTHS  
 437A. CPIWI-NO/CPIWM-NO  
 444. INTERSTATE USE, 100 PERCENT  
 511. DKL300224

Figure 9: Example of TSR to Connect to an Established L3 VPN

**Other Informational Notes:**

**TR Homepage Options**

1. **Copy Existing TR** – 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 – VPN Connections

Users will note that the request for these services is based on the same type actions as ordering SBU IP Data Service (formerly known as NIPRNet). Once the “Connect to a VPN” has been submitted, the other options may be used to “Amend a VPN Connection,” “Change VPN Connection Information,” or “Cancel a VPN Connection.” 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. If you no longer require a VPN connection, the status of your original request to Connect to a VPN will determine which option you must select under “VPN Connections.” If your VPN connection has been established and is active, select the “Discontinue a VPN Connection” option. If your VPN connection has not been established but it is still in the ordering process, select the “Cancel a VPN Connection” option. The “Virtual Private Networks (VPNs)” section actions are addressed in the *Establish a 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 10: Request Action Page for Other Actions

Note when the intent is to “Discontinue a VPN” for an established VPN, users must select the “Discontinue a VPN Connection” for every individual connection established for a particular VPN or “Cancel a VPN Connection” for every individual connection requested that is still in the ordering process. ***All physical connections to that established VPN must be disconnected and/or canceled before a VPN may be discontinued.*** The *Establish a VPN* Customer Ordering Guide provides information on discontinuing an established VPN.

## 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
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	De-Militarized Zone
DoD	Department of Defense
DSS	DISN Subscription Service
DTEN	DISN Test & Evaluation Network
DWCF	Defense Working Capital Fund

Acronym	Term
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
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
NFE	NIPRNet Federated Gateway External
NFG	NIPRNet Federated Gateway
NFI	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
SBU	Sensitive but Unclassified
SGS	SIPRNet GIAP System
SIPRNet	Secret IP Router Network
SLA	Service Level Agreement

Acronym	Term
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)