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 2.0
November 14, 2012

UNCLASSIFIED

Customer Services Division (NS7)
P.O. Box 549
Ft. Meade, MD 20755-0549

This page intentionally left blank.

Signature Page for Key Officials

Approved by:

Signed on November 14, 2012; signature on file	November 14, 2012
Chief, Customer Services Division (NS7)	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

Table of Contents

List of Illustrations

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 new 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 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/DISN-Connection-Process/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	***FUTURE** – DISN Test & Evaluation Network (DTEN – Layer 3 VPN)*
C3	***FUTURE** – SIPRNet Private IP Service (Classified Layer 3 VPN)*
DKL300227	***FUTURE** – Private ISP Service (All Customers – Layer 3 VPN)*
DOL300230	***FUTURE** – IAP Gateway at DECC (All Customers – Layer 3 VPN)*
DKL342000	***FUTURE** – CMNT AR (All Customers – Layer 3 VPN)*
DKCX70001	***FUTURE** – CMNT IPT-PE (All Customers – Layer 2 CsC VPN)*

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), and CX Label Transport Service (Layer 2 CsC 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) 2013. 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), and Label Transport Service (Layer 2 CsC VPN). 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 (NS7)	CML: (800) 554-DISN (3476) or (614) 692-4790 DSN: (312) 850-4790 Global DSN: (510) 376-3222 Unclassified e-mail: DGSC@csd.disa.mil Classified e-mail: DGSC@cols.csd.disa.smil.mil

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.

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.

6.8   CMNT (Layer 3 / Layer 2 VPN)

The Common Mission Network Transport (CMNT) provides an enterprise common transport for Combined Enterprise Regional Information Exchange System (CENTRIXS) encrypted traffic in order to meet mission partners' multi and bilateral communication requirements.

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.

5. 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.
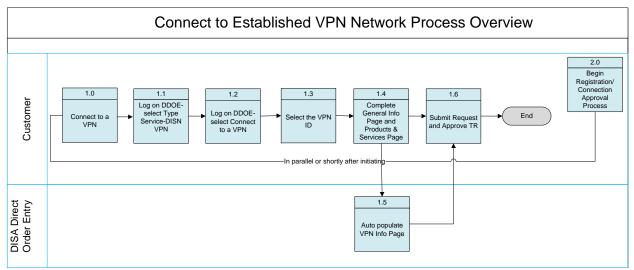

Figure 1: Process to Connect to an Establish VPN

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.

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.*** All the steps and screens for connecting to an established VPN are the same for all the VPN service types (L2, L3, and CX). 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."

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: DISN Virtual Private Network (VPN) ▼

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.

Figure 3: Request Action Page

UNCLASSIFIED

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, 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:

     DISA ▼

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

     VPN ID: DKL300201 - CONUS ▼

(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

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

CJON: WO02MAY124300 TCO Code: WO

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.

(M) Document Classification: UNCLAS

General Information

(M) This requirement is for **DISN Virtual Private Network (VPN)** - **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 elsewhere 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)].

   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

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

CJON: WO02MAY124300 TCO Code: DA

M E N U

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)　｜After The Fact (ATF) or Sooner If Possible (SIP)｜Lead Time Table(s)

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)

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.

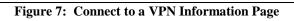   e. **Remarks** – this is an optional field for any remarks information.

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, or CX), 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

❓ M E N U

| 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:	**Ms**				
Last, First MI:	**Turner, Betsy L - Contractor**				
	UNCLAS E-mail				
User E-mail:	UNCLAS E-mail				
Org E-mail:					
	CLASSIFIED E-mail				
User E-mail:					
Org E-mail:					
	Intl Access	Area/Cntry	Exchange	Phone	Extension
Cmcl. Phone:		**301**	**555**	**1234**	

DSN Phone:					
Pager #:					

(R) **Alternate POC**

Rank/Title:	**Ms**				
Last, First MI:	**Badgett, Sheila - Government**				
	UNCLAS E-mail				
User E-mail:					
Org E-mail:	UNCLAS E-mail				
	CLASSIFIED E-mail				
User E-mail:					
Org E-mail:					
	Intl Access	Area/Cntry	Exchange	Phone	Extension
Cmcl. Phone:		**618**	**555**	**1234**	
DSN Phone:					
Pager #:					

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		
	BADGETT	Badgett, Sheila	Defense Information Systems Agency (DISA)	Network Services Directorate - NS
	HENRY	Henry, John	Defense Information Systems Agency (DISA)	Network Services Directorate - NS
	LAKEIN	Lakeinm, Vince	Defense Information Systems Agency (DISA)	DISA CONUS
	LAKE	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, 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, or CX. 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.

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

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

Following is a summary of this request. You are authorized only to view this request. Click Return to return to the TR Home page.

CJON: WO02MAY124300 TCO Code: DA

Request Summary

Funding Line(s)	Service Point(s)
1	1

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

Requester Information			
Rank/Title:	Ms		
Last, First MI:	Turner, Betsy L - Contractor		
Agency:	Defense Information Systems Agency (DISA)		
Organization:	Network Services Directorate - NS		
UNCLAS User E-mail:	email address	**UNCLAS Org E-mail:**	
CLASSIFIED User E-mail:	email address	**CLASSIFIED Org E-mail:**	
Cmcl. Phone:	phone number	**DSN Phone:**	

General Information

Document Classification:	UNCLAS
Type of Service:	DISN Virtual Private Network (VPN) - Private IP Service (Layer 3 VPN)
Geographical Disposition:	CONUS
Request is being submitted on behalf of:	
Agency:	
Organization Account:	DISA (Misc DISA HQ requirements not reflected elsewhere in this table)
Telecommunication Service Priority (TSP) Information	
Provisioning Priority:	NO
Restoration Priority:	NO
Previously authorized TSP Number:	

Product & Service Requirements

Product/Service Description:	Connect to a VPN		
Operational Service Date:	06 Jul 2012	Estimated Service Life:	120 months
Requested CMCL/GFE Service Date:	06 Jul 2012		
Remarks:	Connect to established VPN network		

DISN Virtual Private Network (VPN) Information

VPN ID:	DLL300212
Agency Requiring VPN:	DL - Defense Intelligence Agency - Department of Defense
Type of VPN:	L3 - Private IP Service (Layer 3 VPN)

Primary VPN POC

Name:	Mr. Jack Buck	UNCLAS User E-mail:	email address	UNCLAS Org E-mail:	
CLASSIFIED User E-mail:			CLASSIFIED Org E-mail:		
Cmcl. Phone:	phone	DSN Phone:	phone	Pager:	

Alternate VPN POC

Name:	Ms Betsy L Turner	UNCLAS User E-mail:	email address	UNCLAS Org E-mail:	
CLASSIFIED User E-mail:			CLASSIFIED Org E-mail:		
Cmcl. Phone:	phone	DSN Phone:	phone	Pager:	

VPN TR Routing Information

VPN Routing ID:	DISA01 - DISA VPN MATRIX 1

Technical Information

Type of Operation:	Full Duplex
Do you want DISA to manage your router:	NO
Modulation Rate/Bandwidth:	1.544MB
Service Availability:	Full Period
Signaling Mode:	NO SIGNALING

Funding Information

Overtime/Expedite Charges:		No
Communications Service Authorization (CSA) Number:		New Lease

	Cost Threshold (Not to Exceed)	
Program Designator Code (PDC)	Monthly Recurring Charges (MRC)	Non-Recurring Charges (NRC)
YMTT20	$0.00	$0.00

DISA Cost Estimate

Cost Description	Billing Bandwidth	MRC	NRC
Disclaimer	The TR will be routed to a Provisioning Office for a service cost estimate.		

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.
To DISA Cost Estimate History.

Identification Information

CCSD:	
Agency Code:	D - Defense Information Systems Agency
Purpose/Use:	PN - Private IP Service (Layer 3 VPN)
Type of Service:	G - Permanent Virtual Circuits
Sequence ID:	0001
NSS:	NO - NSS exemption not required.
Jurisdictional Classification:	100 Percent
Is this a BRAC Requirement?	NO
DISA Control Number:	
Exercise/Project Description:	Connect to an established VPN network.
Satellite Data Base (SDB) Approval Number:	

Communications Control Office/Communications Management Office (CCO/CMO) Information

(CCO/CMO) Information:	

Related Request Numbers

CJON(s)/Tracking Number(s):	WO02MAY124300
Work-In-Conjunction With:	

Justification and Approvals

Justification of Service Requested:	
Identification of Reference:	
Approval Document:	
Accreditation Package Information:	

Service Point 1: Herndon, Virginia, United States

Facility Code:	1NJ-DISN NIPRNET DMZ ISOLATION ROUTER - 1ST WITHIN GEOLOC

User Location Information

Address:	1111 Test Drive HERNDON, Virginia 20171-2516	
Building: X	Floor: 1	Room: 101

NPA:	703			NXX:	860
Latitude:				Longitude:	
Directions to Site:	Test				

Primary User POC

Name:	Ms Betsy L Turner - Contractor	UNCLAS User E-mail:	email address	UNCLAS Org E-mail:	
CLASSIFIED User E-mail:				CLASSIFIED Org E-mail:	
Cmcl. Phone:	phone	DSN Phone:	phone	Pager:	

Alternate User POC

Name:	Ms Sheila A Badgett - Government	UNCLAS User E-mail:	email address	UNCLAS Org E-mail:	
CLASSIFIED User E-mail:				CLASSIFIED Org E-mail:	
Cmcl. Phone:	phone	DSN Phone:	phone	Pager:	

Last Half Mile Information

Last Half Mile Site Support Declaration:	No

Service Point #1 Continued

General Service Point Information

Customer Terminal Equipment:	Test
Crypto Equipment:	UNSECURE

Interface Specifications

Physical:	RJ-41
Electrical:	T-1, LINE CODING: B8ZS, FRAME FORMAT: ESF
Detail Interface Information:	Test
Unique On-site Installation Factors:	Test

Inside Wire Requirements

Customer Premise Inside Wire Installation:	No
Customer Premise Inside Wire Maintenance:	No

Security Information

Clearance Required:	Yes
Escort Required:	Yes
Security Instructions:	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:

provttestms@disa.mil	
CC:	
	email address
email address	DISACONTESTIPCMO@disa.mil

Approval Routing List

Sequence	Approver / Office	Status		Comments
1	DISA VPN Office	Pending (notified 02 May 2012 12:52:33)		
2	CONUSTESTIPENG			
3	CONUSTESTENG			
4	DISA Default Office			

Request Summary

Funding Line(s)	Service Point(s)
1	1

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
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
CsC	Carrier supporting Carrier
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
DSS	DISN Subscription Service
DWCF	Defense Working Capital Fund
FY	Fiscal Year
GIAP	GIG Interconnection Approval Process
GIG	Global Information Grid
GNSC	Global NetOps Support Center
IA	Information Assurance
IAP	Internet Access Point

Acronym	Term
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
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
SNAP	System/Network Approval Process
TR	Telecommunications Request
TSR	Telecommunications Service Request
VPN	Virtual Private Network

Defense Information Systems Agency
P.O. Box 549
Ft. Meade, MD 20755-0549
www.disa.mil