Defense Information Systems Agency

A Combat Support Agency

NETWORK SERVICES

VIRTUAL PRIVATE NETWORKS

ESTABLISH AND CONNECT TO A VIRTUAL PRIVATE NETWORK (VPN)

CUSTOMER ORDERING GUIDE

Version 4.0
January 5, 2015

UNCLASSIFIED

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

This page intentionally left blank.

Signature Page for Key Officials

Approved by:

Signature on file

MARTHA O. BUCK
Chief, Business Relationship Management

January 5, 2015

Date

This page intentionally left blank.

Revision History

Version Number	Date	Summary of Changes	Org
1.0	July 2, 2012	Initial release.	NS7
2.0	November 14, 2012	Revised to include a variety of new VPN services and future VPN services. Document renamed and changed to focus on providing guidance and steps to order various VPN services.	NS7
2.1	January 15, 2013	Revised to include differences in ordering associated with Private ISP Service and IAP Gateway at DECC.	NSP4
2.2	January 25, 2013	Added DTEN type available now. Ensure references consistent throughout doc. Updated acronyms.	NSP4
2.3	March 7, 2013	Added NIPRNet Federated Gateway.	NSP4
2.4	March 12, 2013	Updated links to Enterprise Connection. Prepared for release to external mission partners.	NSP4
2.5	May 6, 2013	Update to add availability of MED COI and CMNT COI.	NSP4
3.0	August 14, 2013	Update to note DGSC email address change, change name from DTEN to DTES, add availability Quality of Service (QoS), and provide information for Private Data ISP Service IP address space requirements.	NSP4
3.0	September 6, 2013	Final review edits.	NSP4
3.1	October 2, 2013	Update note on DTES CNDSP.	NSP4
4.0	January 5, 2015	Updated to add CCSA to IAP DMZ, and add JIE-JRSS. Updates to VPN service types. Annual review. Combined Establish a VPN and Connect to an Established VPN Customer Ordering Guides. Updates to ensure document is OPSEC compliant. Reviewed VPN service descriptions, and added option to have a virtual or physical connection. Added DSAWG required statements for Private Data ISP. Added DSAWG requirements and/or approval required prior to being granted Permission to Connect to the DISN to the business rules sections. General editing.	BRM

Table of Contents

List of Illustrations

1. Introduction

The Defense Information Systems 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 IP services fall within the DISN Subscription Service (DSS) structure. This document outlines procedures for ordering VPN services available either now or in the near future, and announces the implementation of Quality of Service (QoS) for specific VPN service types. The VPN services and VPN Identifiers (VPN IDs) are listed in Table 1. Detailed service descriptions are provided in Section 6, VPN Service Descriptions.

The process and detailed information to order these services, which requires two steps, are provided in this VPN Ordering Guide. The first step is to ***Establish a VPN*** and the second step is to ***Connect to a VPN***. Guidance for registering Sensitive but Unclassified (SBU) VPNs in the System/Network Approval Process (SNAP) database is provided in the VPN SNAP Registration Guide, available at http://disa.mil/Services/Network-Services/Enterprise-Connections/Connection-Process-Guide/Service-Appendices/VPN-Registration-Private-IP and https://snap.dod.mil. In addition, the appendices of the Connection Process Guide (CPG) provide registration instructions for unclassified VPN services in SNAP. Electronic and print versions of the CPG can be accessed at http://www.disa.mil/Services/Network-Services/Enterprise-Connections/Connection-Process-Guide. Guidance for registering classified VPNs in the Secret Internet Protocol Router Network (SIPRNet) Global Information Grid (GIG) Interconnection Approval Process (GIAP) System (SGS) is provided in the SGS Registration Guide, available at https://www.disa.smil.mil/connect and https://giap.disa.smil.mil.

VPN ID/Code	Service Name
L3	Private IP Service (Layer 3 VPN)
L2	Private Local Area Network (LAN) Service (Layer 2 VPN)
C3	Secret Private IP Service (Classified Layer 3 VPN)
CX	Label Transport Service (Layer 2 Carrier Supporting Carrier (CsC) VPN)
TE	DISN Test and Evaluation Service (DTES) (Layer 3 VPN)
DKL300251	Medical Community of Interest (Med COI) Service for the Defense Medical Information Exchange (DMIX) (Layer 3 VPN) – *Authorized "Medical Community Only" users of the Department of Defense (DoD) and Department of Veterans Affairs (VA); mission partners can only submit "Connect to VPN" requests for this service. DISA Control Number (DCN) code for this service is D314.*
DKL342000	Coalition Mission Network Transport (CMNT) Community of Interest (COI) (Layer 3 VPN) – *Mission partners can only submit "Connect to VPN" requests for this service*
DKL300227	Private Data Internet Service Provider (ISP) Service (All mission partners – Layer 3 VPN) – *Mission partners can only submit "Connect to VPN" requests for this service*
DOL300230	Internet Access Point (IAP) Demilitarized Zone (DMZ) (All mission partners – Layer 3 VPN) – *Mission partners can only submit "Connect to VPN" requests for this service*

VPN ID/Code	Service Name
DKL300249	Mission Partner Gateway (MPG) COI (All mission partners – Layer 3 VPN) (formerly known as MPG/NIPRNet Federated Gateway (NFG)) – *Mission partners can only submit "Connect to VPN" requests for this service*
DKCX70010	Joint Information Environment (JIE)–Joint Regional Security Stack (JRSS) COI (All mission partners – Layer 2 VPN) – *Mission partners can only submit "Connect to VPN" requests for this service*

Table 1: VPN Services

Note 1: More VPN IDs may be added in the future.
Note 2: In accordance with a recent DISA directive, "mission partner" is synonymous with "customer" throughout this document.

The above-described VPN services are available for ordering via the Defense Information Systems Agency (DISA) Direct Order Entry (DDOE), with the following exceptions: C3 – Secret Private IP Service (Classified Layer 3 VPN); DOL300230 – IAP DMZ (all mission partners – Layer 3 VPN); DKL300249 – MPG COI (all mission partners – Layer 3 VPN); DKL300227 – Private Data ISP Service (all mission partners – Layer 3 VPN); and DKCX70010 – JIE-JRSS COI (all mission partners – Layer 2 VPN). These remaining VPN services will be available in calendar year (CY) 2015. To announce the availability of these services, a Business Service Catalog (BSC) Customer Notice will be posted on the DISA website at http://www.disa.mil/Services/Network-Services, and an announcement will be posted on the DISA Direct homepage at https://www.disadirect.disa.mil/products/ASP/welcome.ASP.

2. Purpose

This guide provides detailed information necessary to ***Establish a VPN*** and to ***Connect to VPN*** via DDOE for available VPN services noted in Table 1. It also includes minor differences in ordering associated with Private Data ISP Service, Internet Access Point (IAP) Demilitarized Zone (DMZ), Coalition Mission Network Transport (CMNT) Community of Interest (COI) (now Layer 3 VPN only), Medical COI (Med COI) for Defense Medical Information Exchange (DMIX), Mission Partner Gateway (MPG) COI, and Joint Information Environment (JIE) – Joint Regional Security Stack (JRSS) COI VPN services.

This document assumes the reader has basic familiarity with DDOE and an established account with role(s). The DISA Direct homepage can be accessed at the link provided above. New functionality in DDOE has been added to allow users to change an existing connection to an established VPN ID.

3. References

a. Network Services, Virtual Private Networks, Establish a Virtual Private Network (VPN) Customer Ordering Guide, Version 3.1, October 2, 2013 (canceled).

b. Network Services, Virtual Private Networks, Connect to an Established Virtual Private Network (VPN) Customer Ordering Guide, Version 3.1, October 2, 2013 (canceled).

c. Network Services, Virtual Private Network (VPN) SNAP Registration Guide, Version 1.4, January 5, 2015.

d. Network Services, Virtual Private Network (VPN) SGS Registration Guide, Version 1.0, March 14, 2014.

e. Enterprise Connection Division Defense Information Systems Network (DISN) Connection Process Guide (CPG), Version 5.0, November 2014.

f. DISA Circular (DISAC) 310-65-1, Channel and Circuit Allocation, April 4, 2014.

g. DoD Instruction (DoDI) 8110.1, Multinational Information Sharing Networks Implementation, February 6, 2004.

h. Action Memo, Secretary of Defense, Subject: Integrated Electronic Health Record (iEHR) Medical Community of Interest (Med COI), February 25, 2013.

i. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02D, Defense Information Systems Network (DISN) Responsibilities, January 24, 2012.

4. Roles and Responsibilities

It is the mission partner’s responsibility to order VPN services as deemed necessary and to ensure registration within the SNAP and SGS databases.

5. Points of Contact

For additional information, help with DDOE, or assistance with ordering VPN services, contact the DISN Global Support Center (DGSC) using the information provided in Table 2.

DGSC	
Business Relationship Management (BRM)	DSN: (312) 850-4790 CML: (800) 554-3476 or (614) 692-4790 SBU IP Data e-mail: dgsc@csd.disa.mil Secret IP Data e-mail: disa.columbus.ns.mbx.dgsc@mail.smil.mil

Table 2: Points of Contact

6. VPN Service Descriptions

6.1 Private Internet Protocol (IP) Service (Layer 3 VPN)

This VPN service enables mission partners 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 mission partners across the DISN. This service is available as part of the DSS Cost Recovery Model at any DSS location that includes Sensitive but Unclassified Internet Protocol Data (SBU IP Data) Service. Private IP service will enable mission partners 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. Service can be ordered with a physical or virtual connection to the DISN. Virtual connection requires specific hardware; mission partners can contact the DGSC to inquire about hardware limitations to determine whether they can support virtual interface functionality.

6.2 Private Local Area Network (LAN) Service (Layer 2 VPN)

This VPN service provides mission partners the ability to shrink the world to one 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 Multiprotocol Label Switching (MPLS) IP 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 mission partner LANs to create a single bridged LAN. Private LAN Service provides segmented IP service for mission partners utilizing an MPLS Layer 2 VPN.

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

6.3 Label Transport Service (Layer 2 VPN)

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

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

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

Test and Evaluation (T&E) IP data (operating over the DTEN, known as the DISN T&E Network) is part of the DSS Cost Recovery Model. This VPN service provides a black transport capability riding the DISN backbone. It offers standard DISN services and Service Level Agreements (SLAs) to DTES mission partners. The COIs are responsible for their Computer Network Defense Service Provider (CNDSP) services; this falls outside of DISA's management boundaries. DISA will not be responsible for COI mission partners' CNDSPs, or for mission partners' Communications Security (COMSEC). Service can be ordered with a physical or virtual connection to the DISN. Virtual connection requires specific hardware and mission partners can contact the DGSC to inquire about hardware limitations to determine if they can support virtual interface functionality.

6.5 Secret Private IP Service (Classified Layer 3 VPN)

This VPN service enables mission partners' 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 mission partners across the Secret IP Data Service. This service is available as part of the DSS Cost Recovery Model at any DSS location that includes Secret IP Data Service. Secret Private IP Service provides segmented IP service for mission partners utilizing an MPLS Layer 3 VPN and requires a separate physical interface for each connection.

6.6 Private Data Internet Service Provider (ISP) Service (Layer 3 VPN)

This VPN service provides mission partners the ability to obtain Internet access through an MPLS Layer 3 VPN at any DISN IAP. Private Data ISP Service is an enterprise VPN service providing ISP access to mission partners across the DISN. Service is available as part of the DSS Cost Recovery Model at any DSS location that includes SBU IP Data Service. Circuit accreditation is significantly faster and requires less paperwork to complete. Service requires mission partner to order virtual connection to the DISN. Virtual connection requires specific hardware; mission partners can contact the DGSC to inquire about hardware limitations to determine whether they can support virtual interface functionality.

This VPN is "established" by DISA. Mission partners can only submit Telecommunications Requests (TRs) in DDOE to "Connect to VPN"; the VPN ID is DKL300227.

In addition, mission partners will be required to request IP address space from the DoD Network Information Center (NIC) for their connection to work with Private Data ISP Service. Customers must obtain the IP address space out of the reserved IP space for Private Data ISP Service: 139.241.0.0/16. Refer to Section 8.2, Business Rules, for specific IP address space ordering information and instructions.

To obtain Permission to Connect (PTC) approval from DISA for Private Data ISP Service, the mission partner must submit an Authority to Operate (ATO) from their Designated Approving Authority (DAA) containing the following statement:

No ingress or egress restrictions are provided by DISA. DAA understands that this service has no Computer Network Defense (CND) or firewall protections, and the DAA is assuming the risk associated with an open Internet connection.

The ATO also must include:

a. The Command Communications Service Designators (CCSDs) of the two virtual circuits must be in the subject line of the ATO.

b. The IP address space assigned by the DoD NIC must be included in the ATO.

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

This VPN service provides mission partners the ability to obtain Internet access through an MPLS Layer 3 VPN at any Combatant Command, Service, Agency, or Field Activity (CC/S/A/FA) or Defense Enterprise Computing Center (DECC) location to access any DISN IAP. IAP DMZ service is an enterprise VPN service providing IAP Internet access to mission partners across the DISN. This service is available as part of the DSS Cost Recovery Model at any DSS location that includes SBU IP Data Service.

This service provides for logical and physical isolation of public-facing Internet applications at DoD CC/S/A/FA-provided DMZ locations. IAP DMZ service is an implementation of MPLS VPN to move traffic across the DISN from IAP to DMZ extension, and then using Virtual Routing and Forwarding (VRF) and virtual firewalling techniques to terminate the COI connection at an enclave boundary. Service can be ordered with a physical or virtual connection to the DISN. Virtual connection requires specific hardware; mission partners can contact the DGSC to inquire about hardware limitations to determine whether they can support virtual interface functionality.

This VPN is “established” by DISA. Mission partners can only submit TRs in DDOE to “Connect to VPN”; the VPN ID is DOL300230. DDOE will assign this VPN ID to all mission partners requesting IAP DMZ service. Mission partners must use DISA Control Number (DCN) D316 when submitting requests to connect to this service.

NOTE: IAP DMZ service is an “Internet only” service. Mission partners ordering this service will be connected to the DISN but will only have access to the World Wide Web. No access to DoD networks is available. All orders for this service will be marked with DCN D316.

6.8 Mission Partner Gateway (MPG) Community of Interest (COI) (Layer 3 VPN)

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

Gateway External (NFE) Router" and "External Customer on SBU IP Data Service"). The system shall support logical traffic separation as traffic transits through the SBU IP Data Service.

This service is for non-DoD federal agencies and mission partner connections that connect directly into the SBU IP Data Service. Mission partners ordering this service will be connected to the DISN but will have their connection directed to the nearest MPG NFE router. All traffic will go through the NFE prior to accessing any DoD available networks. Service can be ordered with a physical or virtual connection to the DISN. Virtual connection requires specific hardware; mission partners can contact the DGSC to inquire about hardware limitations to determine whether they can support virtual interface functionality.

MPG mission partners can be categorized into two types:

1. External Mission Partner 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 Internet Access Point Network (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 mission partner equipment may be collocated with an MPG site and with back-to-back connections with the router. With these types of connections, encryption may not be necessary. These mission partners may use External Border Gateway Protocol (eBGP) peers directly with the NFE router on the physical interface using the interface IP address.

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

VPN naming conventions, as defined in DISAC 310-65-1, were used to obtain the VPN ID for the MPG COI (formerly known as MPG/NIPRNet Federated Gateway (NFG)). The VPN ID for MPG COI service is provided by DISA and will always be the same for every mission partner.

This VPN is "established" by DISA. Mission partners can only submit TRs in DDOE to "Connect to VPN"; the VPN ID is DKL300249. Mission partners must use DCN D212 when submitting requests to connect to this service.

6.9 Coalition Mission Network Transport (CMNT) COI (Layer 3 VPN)

The CMNT COI provides a distinct and common transport for Combined Enterprise Regional Information Exchange System (CENTRIXS) traffic in order to meet mission partners' multilateral and bilateral communication requirements. CMNT will separate the CENTRIXS coalition networks (enclaves) from the Secret IP Data Service, thereby eliminating CENTRIXS' dependence on Secret IP Data Service for transport. This requirement supports DoDI 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 mission partners the ability to obtain 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 mission partners across the DISN. This service is available as part of the DSS Cost Recovery Model at any DSS location that includes IPT-PE IP Data access. CAP accreditation is significantly faster and requires less paperwork to complete. Service can be ordered with a physical or virtual connection to the DISN. Virtual connection requires specific hardware; mission partners can contact the DGSC to inquire about hardware limitations to determine whether they can support virtual interface functionality.

The VPN naming convention was used to obtain the VPN ID for CMNT VPN service. The VPN ID for CMNT VPN service is provided by DISA and will always be the same for every CMNT mission partner.

This VPN is "established" by DISA. Mission partners can only submit TRs in DDOE to "Connect to VPN"; the VPN ID is DKL342000 (Layer 3 VPN). DDOE will assign this VPN ID to all CMNT mission partners requesting CMNT VPN service.

NOTE: CMNT VPN service is a "mission partner/Combatant Command (COCOM) only" service. Mission partners ordering this service will be connected to the DISN but will not have access to the World Wide Web, SBU IP Data Service, or Secret IP Data Service. No access to DoD networks is available. This is a restricted access service, and all requests to connect to this service must be verified and approved by DISA.

6.10 Medical COI (Med COI) Service for Defense Medical Information Exchange (DMIX) (Layer 3 VPN)

Med COI Service for the DMIX is a VPN service that provides mission partners 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 DoD and Department of Veterans Affairs (VA). The DoD and/or VA Med COI approving authority must authorize connection to this VPN. This service is available as part of the DSS Cost Recovery Model at any DSS location that includes SBU IP Data Service. CAP accreditation is required, and the process is significantly faster and requires less paperwork to complete. Service can be ordered with a physical or virtual connection to the DISN. Virtual connection requires specific hardware; mission partners can contact the DGSC to inquire about hardware limitations to determine whether they can support virtual interface functionality.

The Med COI for DMIX VPN has been established under the authority of the Secretary of Defense Action Memo dated February 25, 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 mission partner. Mission partners can only submit TRs in DDOE to "Connect to VPN"; the VPN ID for Med COI Service for DMIX (Layer 3 VPN) is DKL300251. DDOE will assign this VPN ID to all mission partners requesting Med COI Service. The DCN for this service is D314. DDOE will automatically populate all Med COI orders with this DCN.

NOTE: Med COI Service is a "medical community only" service. Mission partners 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.

6.11 Joint Information Environment (JIE) – Joint Regional Security Stack (JRSS) COI (Layer 2 VPN)

The JIE-JRSS COI VPN is to provide MPLS Labeled Service to all Joint Router-Customer Edge (JR-CE) and Joint Base-Customer Edge (JB-CE) routers. This will allow these Customer Edge (CE) routers to be a single MPLS domain. The IPT-PE will essentially look like P routers to these CE routers, so the CE routers can provide MPLS VPNs to support all JRSS traffic flow.

This VPN service is available as part of DSS at any DSS location that includes IP Data access. CAP accreditation is significantly faster and requires less paperwork to complete. Service can be ordered with a physical or virtual connection to the DISN. Virtual connection requires specific hardware; mission partners can contact the DGSC to inquire about hardware limitations to determine whether they can support virtual interface functionality.

The VPN naming convention was used to obtain the VPN ID for JIE-JRSS VPN service. The VPN ID for JIE-JRSS VPN service is provided by DISA and will always be the same for every JIE-JRSS COI mission partner. The JIE-JRSS COI VPN service VPN ID is DKCX70010. DDOE will assign this VPN ID to all JIE-JRSS COI mission partners requesting service.

NOTE: JIE-JRSS COI service is an enterprise service offering. Mission partners ordering this service will connect to the DISN but will be routed to the JRSS prior to being given access to any other DISN assets such as the World Wide Web, NIPRNet, or SIPRNet. This is a restricted access service, and all requests to connect to this service will be verified and approved by DISA.

7. Establish a VPN (Step 1)

7.1 Process Overview

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

1. The DDOE process is used to establish a VPN.

2. An authorized DDOE user logs into DDOE and selects the type of service (i.e., DISN Virtual Private Network (VPN)) and "Establish a Virtual Private Network (VPN)."

3. A VPN Point of Contact (POC) will be designated. An Alternate POC also may be designated.

4. A VPN Name/Number will be generated by DDOE in accordance with DISAC 310-65-1 naming conventions. Mission partners will receive feedback indicating successful action and providing the VPN Name/Number to be used when ordering connections (see Section 8, Connect to a VPN (Step 2)).

Figure 1 depicts the process overview to establish a VPN. Business rules and specific steps are detailed in subsequent sections of this document.

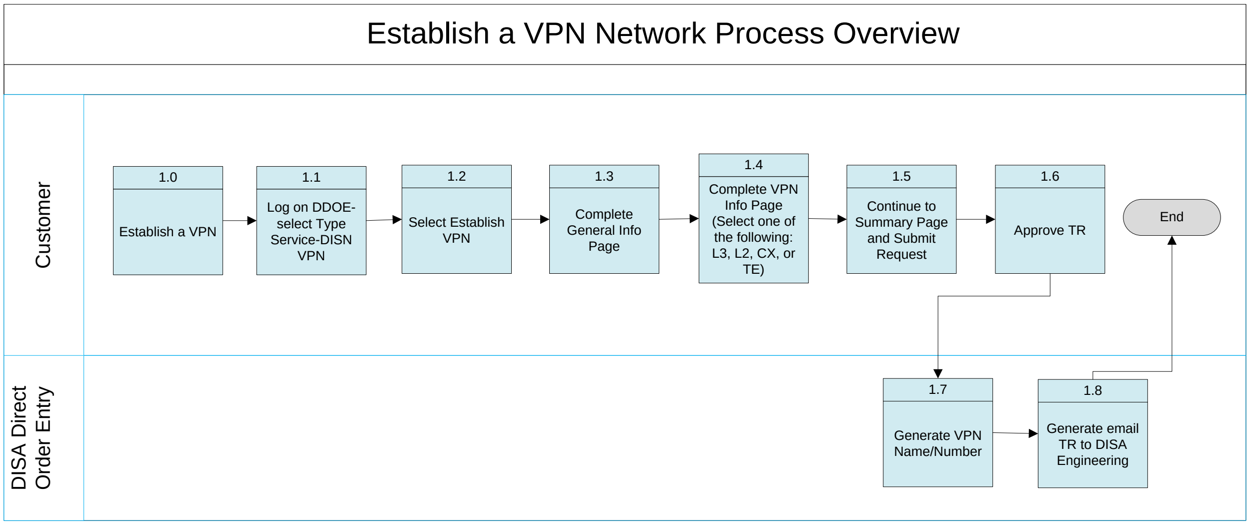

Establish a VPN Network Process Overview
Customer
DISA Direct Order Entry
1.0
Establish a VPN
1.1
Log on DDOE-select Type Service-DISN VPN
1.2
Select Establish VPN
1.3
Complete General Info Page
1.4
Complete VPN Info Page (Select one of the following: L3, L2, CX, or TE)
1.5
Continue to Summary Page and Submit Request
1.6
Approve TR
End
1.7
Generate VPN Name/Number
1.8
Generate email TR to DISA Engineering

Figure 1: Process to Establish a VPN

7.2 Business Rules

Ordering of DISN VPNs is based on the premise and template for ordering SBU IP Data Service. Additional business rules apply when ordering these services.

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

2. The action types that apply to ***Establish a VPN*** are as follows: Establish a VPN, Change VPN Point of Contact (POC) Information, and Discontinue a VPN. These actions are performed on the VPN (network) itself, vice individual connections to the established VPN. The following rules apply when establishing a VPN. Table 1 identifies specific VPN types that are DISA-established VPNs. Mission partners cannot establish these VPN types but can only request connections to the DISA-established VPN types.

    a. Funding requirements are in accordance with the business rules for the DSS Cost Recovery Model.

    b. No TSR will be generated.

    c. An e-mail is sent to the applicable engineering e-mail address, the originator, and/or all POCs, as well as to any added e-mail addresses, upon final approval of the TR. The action e-mail address of the engineering e-mail is based on the geographical disposition selection made on the Establish a VPN TR.

    d. The full VPN ID will be generated automatically upon final approval of the TR. This identifier will be needed in order to submit request for connect to VPN.

    e. TR routing for this type of request is based on a new routing identifier, the VPN Routing ID. Setup and maintenance will be part of the Request Routing application and are the responsibility of the agency's Routing List Official (RLO).

    f. To discontinue an established VPN (network), all individual physical/virtual VPN connections to that network must be disconnected first.

    g. The agency's RLO utilizes the Request Routing application to set up and maintain the VPN Routing ID. All of the agency's VPN Routing IDs that have been set up by the RLO are automatically presented on the TR page for selection when establishing a VPN.

3. QoS Implemented – QoS is the ability to provide different priorities to different pre-marked packets (applications, users, or data flows) or to guarantee a certain level of performance to those packets across the DISN. It does not give one mission partner's traffic a higher priority than another mission partner's traffic.

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

    Effective immediately, the TR will auto-populate the type of QoS template. The following types of service offerings will reflect QoS General Transport Path (GTP): DISN VPN

(Private IP Service) (Layer 3 VPN) - L3, Private LAN Service (Layer 2 VPN) - L2, and Label Transport Service (Layer 2 CsC) - CX. The QoS template code will be reflected automatically in TSR Item 142. Service offerings not listed here will not reflect QoS.

4. The CJCSI 6211.02D, Enclosure D, paragraph 15, states that Defense IA Security Accreditation Working Group (DSAWG) approval must be obtained "before tunneling classified data across unclassified IP infrastructure." DSAWG has granted DISA approval authority for tunneling classified traffic over unclassified MPLS routers if the following conditions are met.

   a. The DAA ATO letter must have the following statement:

      The DAA understands that classified information sent to DISA will be Type 1 or Suite B cryptography encrypted prior to transmission and traffic is routed by the DISN unclassified router network.

   b. Connection will be on a dedicated physical interface on the DISN unclassified router. NOTE: Virtual interfaces will be permitted when testing has been completed and Configuration Control Board (CCB) approval has been granted (expected in March or April 2015).

   c. There are no backdoor connections (NIPRNet, SIPRNet, etc.).

   d. The standard QoS 6 queue model is applicable.

   e. Detailed topology showing all connections is required.

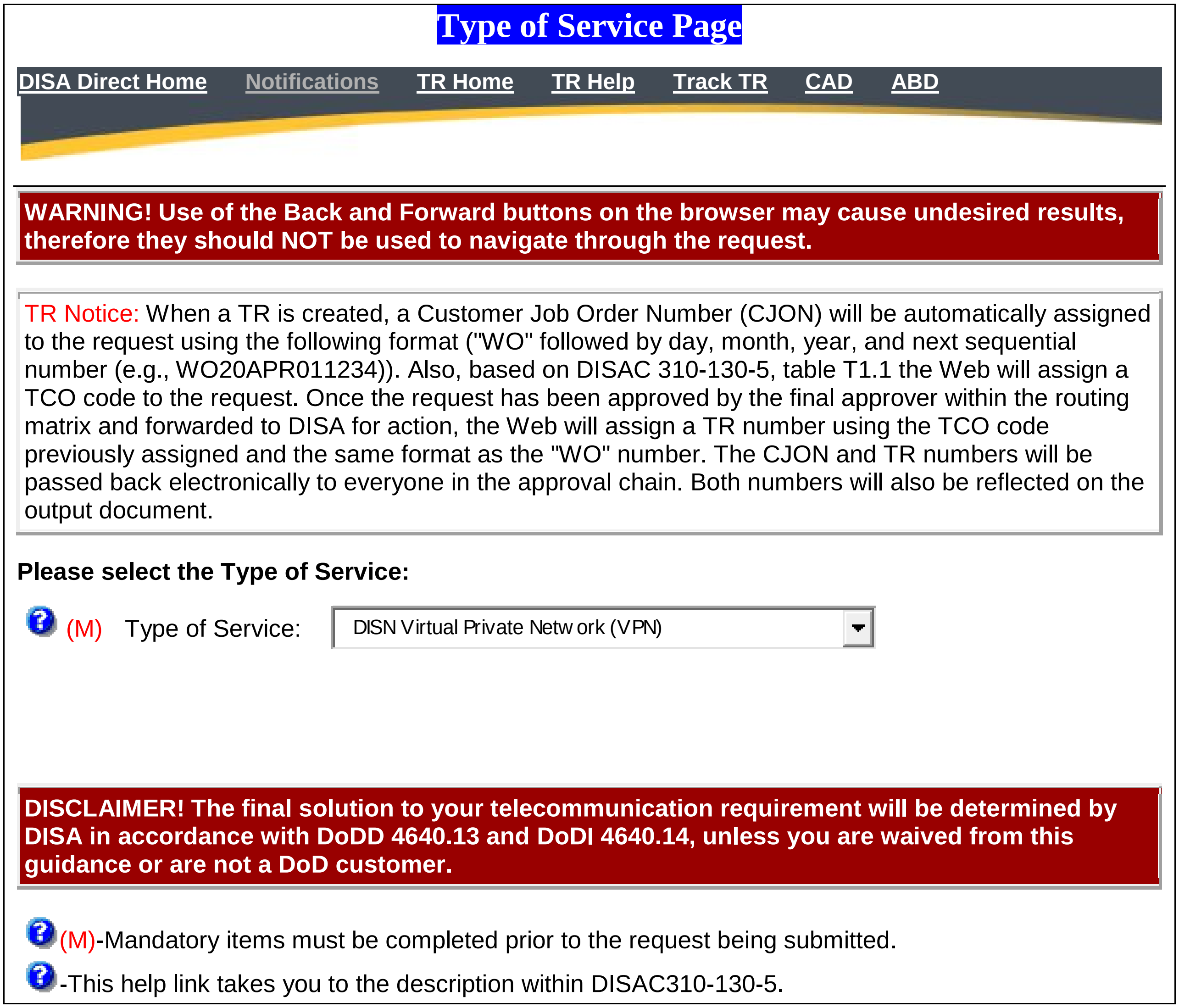
   Any connections that do not meet the above requirements must have DSAWG approval prior to being granted PTC to the DISN.

7.3 Steps to Establish a VPN on DDOE

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

See Table 1 for specific VPN types that are DISA-established VPNs. Mission partners cannot establish these VPN types; they can only request connections to the DISA-established VPN types.

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

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.

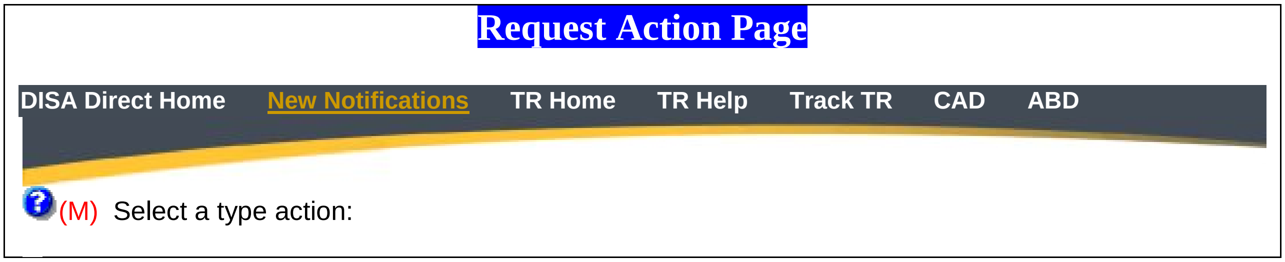
(M)-Mandatory items must be completed prior to the request being submitted.

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

Figure 2: Type of Service Page

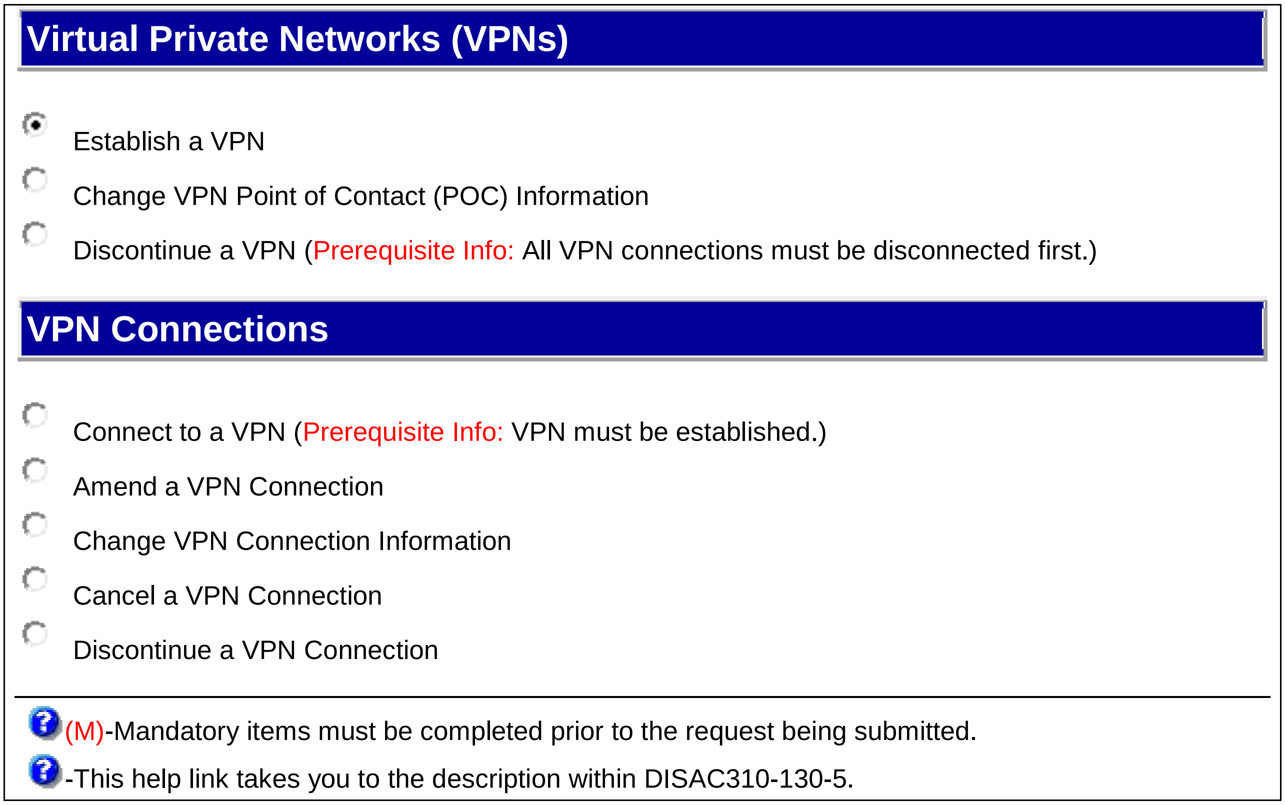
ACTION: ARO/APO selects “Establish a VPN” for the request action under “Virtual Private Networks (VPNs),” as shown below.

NOTE: This action type is *NOT* available for DISA-established VPN types (see Table 1). Mission partners can only request a connection to these VPN types.



Request Action Page

(M) Select a type action:



Virtual Private Networks (VPNs)

● Establish a VPN

○ Change VPN Point of Contact (POC) Information

○ Discontinue a VPN (Prerequisite Info: All VPN connections must be disconnected first.)

VPN Connections

○ Connect to a VPN (Prerequisite Info: VPN must be established.)

○ Amend a VPN Connection

○ Change VPN Connection Information

○ Cancel a VPN Connection

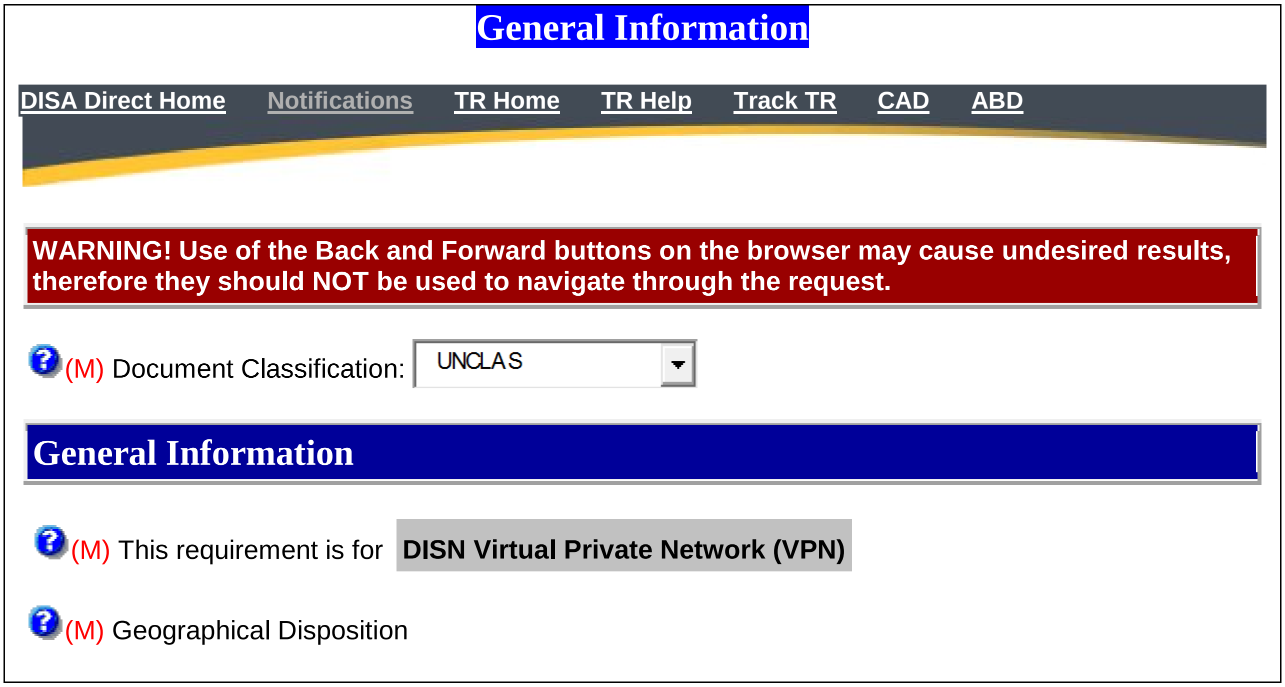
○ Discontinue a VPN Connection

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

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

Figure 3: Request Action Page

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



General Information

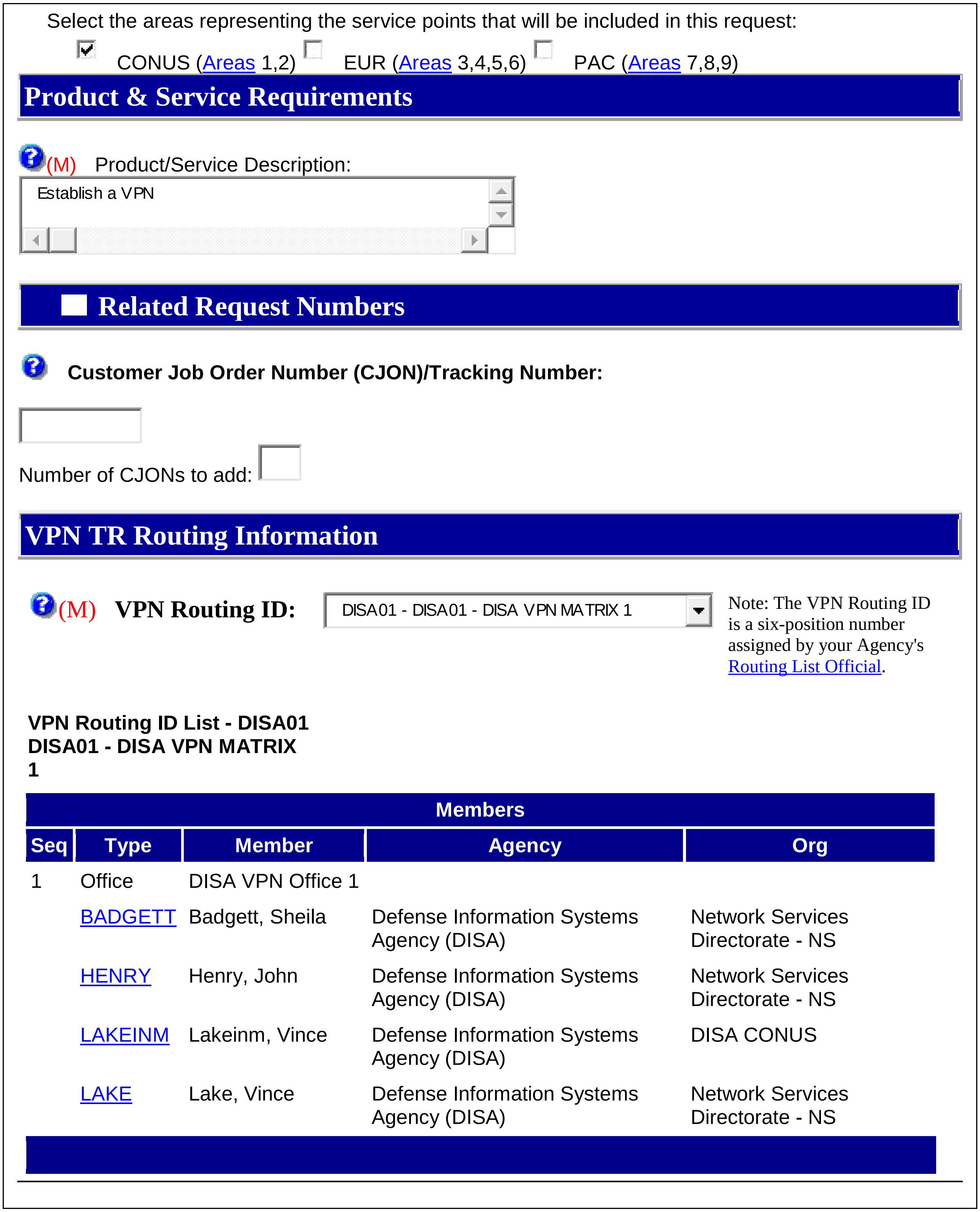
WARNING! Use of the Back and Forward buttons on the browser may cause undesired results, therefore they should NOT be used to navigate through the request.

? (M) Document Classification: UNCLAS ▾

General Information

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

? (M) Geographical Disposition



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

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

Product & Service Requirements

(M) Product/Service Description:

Establish a VPN

Related Request Numbers

Customer Job Order Number (CJON)/Tracking Number:

Number of CJONs to add:

VPN TR Routing Information

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

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

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

Members				
Seq	**Type**	**Member**	**Agency**	**Org**
1	Office	DISA VPN Office 1		
	BADGETT	Badgett, Sheila	Defense Information Systems Agency (DISA)	Network Services Directorate - NS
	HENRY	Henry, John	Defense Information Systems Agency (DISA)	Network Services Directorate - NS
	LAKEINM	Lakeinm, Vince	Defense Information Systems Agency (DISA)	DISA CONUS
	LAKE	Lake, Vince	Defense Information Systems Agency (DISA)	Network Services Directorate - NS

Figure 4: General Information Page

General Information Page – VPN Details:

1. **General Information** – This section automatically displays the service type name (e.g., DISN Virtual Private Network (VPN)).

   a. **Geographical Disposition** – Mandatory selection to indicate the area. Select one or more of the areas that represent the VPN location.

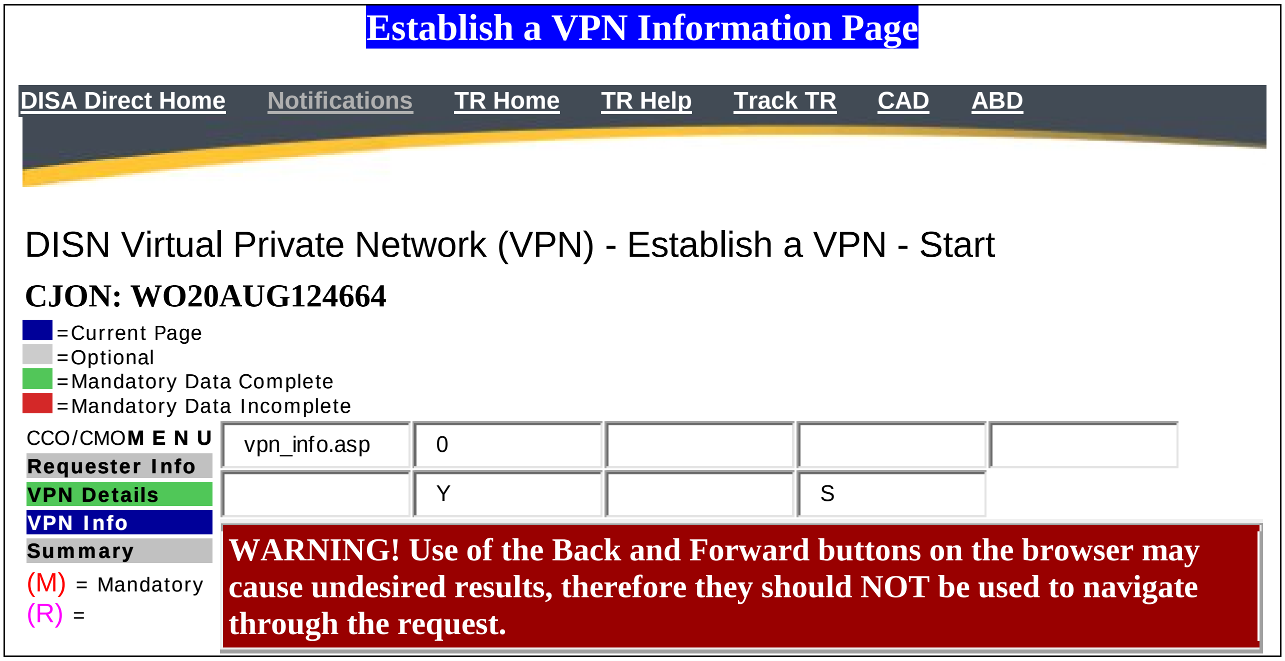
2. **Product & Service Requirements** – This mandatory text field will automatically populate with the type of action selected: Establish a VPN. Additional product/service description information may be added.

3. **Related Request Numbers** – This section is optional on all TRs and allows additional Customer Job Order Numbers (CJONs) to be added to track the requirement.

4. **VPN TR Routing Information** – Establishing a VPN does not require funding using the Program Designator Code (PDC). However, to coordinate the service request, a VPN Routing ID is used. The agency RLO is responsible for setting up and maintaining VPN Routing IDs. All VPN routing IDs that the RLO has set up will be presented automatically in the VPN Routing Information section. If no VPN Routing IDs are shown, or if a new VPN Routing ID is required, the RLO hyperlink should be selected to contact your agency's RLO. NOTE: Mission partners must provide funding for any access circuit to a non-DSS subscription site if required.

   a. **VPN Routing ID** – Mandatory selection.

ACTION: ARO/APO completes the "Establish a VPN Information Page," as shown below, selecting the type of VPN (e.g., L2, L3, TE, CX, etc.) and clicks "Continue."



Establish a VPN Information Page

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

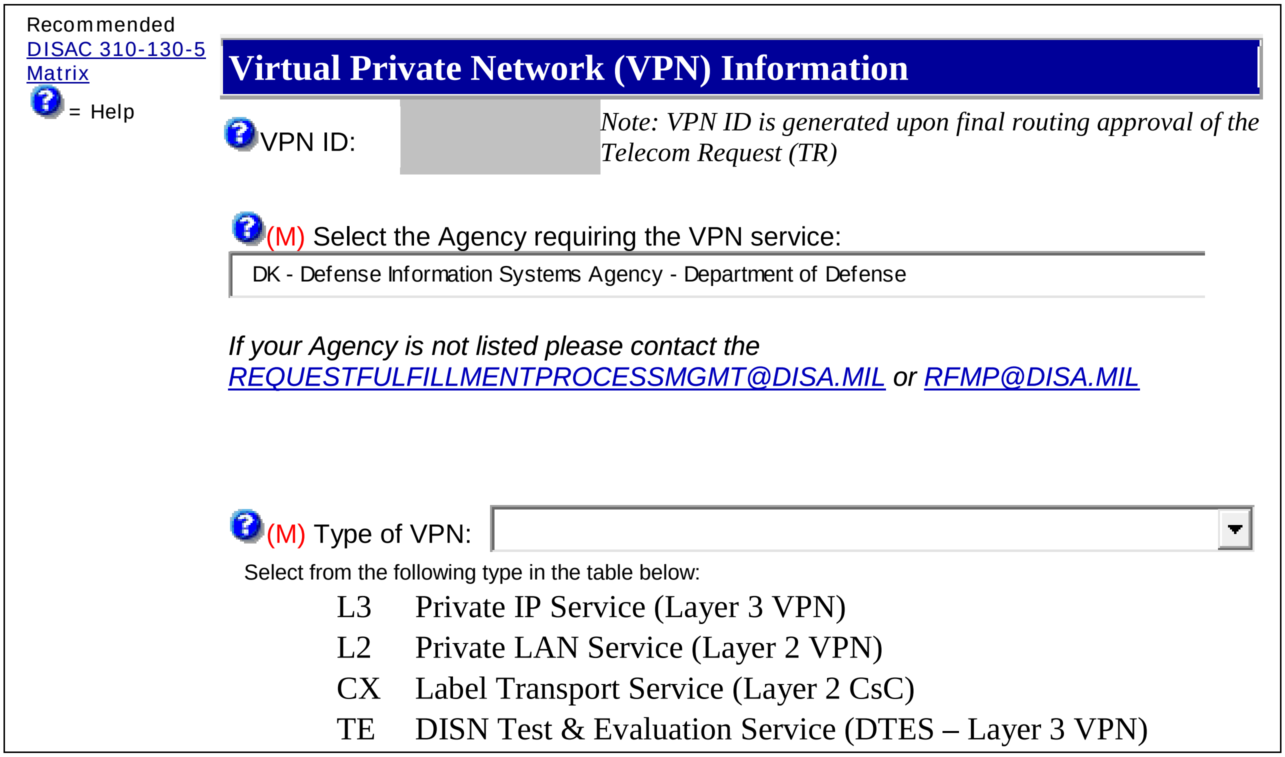
CJON: WO20AUG124664

🟦 =Current Page
⬜ =Optional
🟩 =Mandatory Data Complete
🟥 =Mandatory Data Incomplete

(M) = Mandatory
(R) =

vpn_info.asp	0			
	Y		S	

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.



Recommended
DISAC 310-130-5 Matrix
? = Help

Virtual Private Network (VPN) Information

? VPN ID:

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

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

DK - Defense Information Systems Agency - Department of Defense

If your Agency is not listed please contact the REQUESTFULFILLMENTPROCESSMGMT@DISA.MIL or RFMP@DISA.MIL

? (M) Type of VPN: ▼

Select from the following type in the table below:

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

Figure 5: Establish a VPN Information Page

Establish a VPN Information Page:

1. **Virtual Private Network (VPN) Information** – This section provides the VPN ID, the agency requiring the service, and the type of VPN.

   a. **VPN ID** – This is a display field. The VPN ID is generated upon final routing approval of the TR.

   b. **Select the Agency Requiring the VPN Service** – Select the agency that requires the VPN service; this is a mandatory selection. The agency code and description are based on DISAC 310-65-1, Chapter 3, "Agency Requiring the Service," paragraph C3.4, "Listing of Codes." If the agency is not listed, select the content e-mail provided (hyperlinked e-mail address on the page) to send an email to request the agency name to be added.

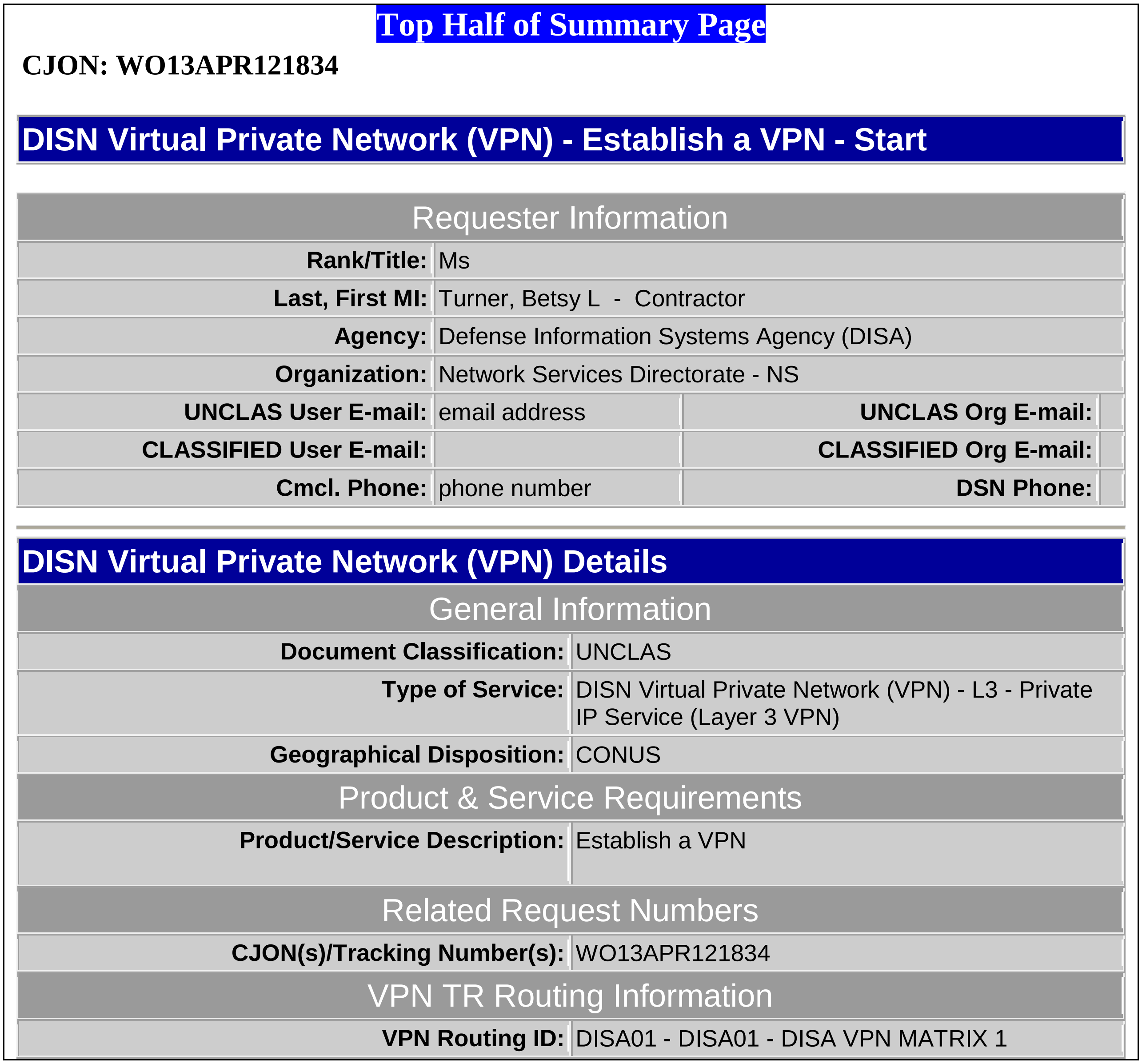
   c. **Type of VPN** – The type of VPN service is available in the drop-down menu for L2, L3, CX, or TE. The examples provided below are for the "L3 - Private IP Service (Layer 3 VPN)" type of VPN.

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

   a. **Primary POC** – Selection of a Primary POC is mandated in order to identify a POC at the VPN location. The POC selection information is accessed by selecting "Retrieve/Enter POC Information" or "Retrieve/Enter Special POC Information." The user retrieves the mandatory Primary POC information by searching the Central Address Directory (CAD).

b. **Alternate POC** – Selection of an additional POC at the VPN site is highly recommended in case the Primary POC is not available. POC selection information is accessed by selecting “Retrieve/Enter POC Information” or “Retrieve/Enter Special POC Information.”

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



Top Half of Summary Page

CJON: WO13APR121834

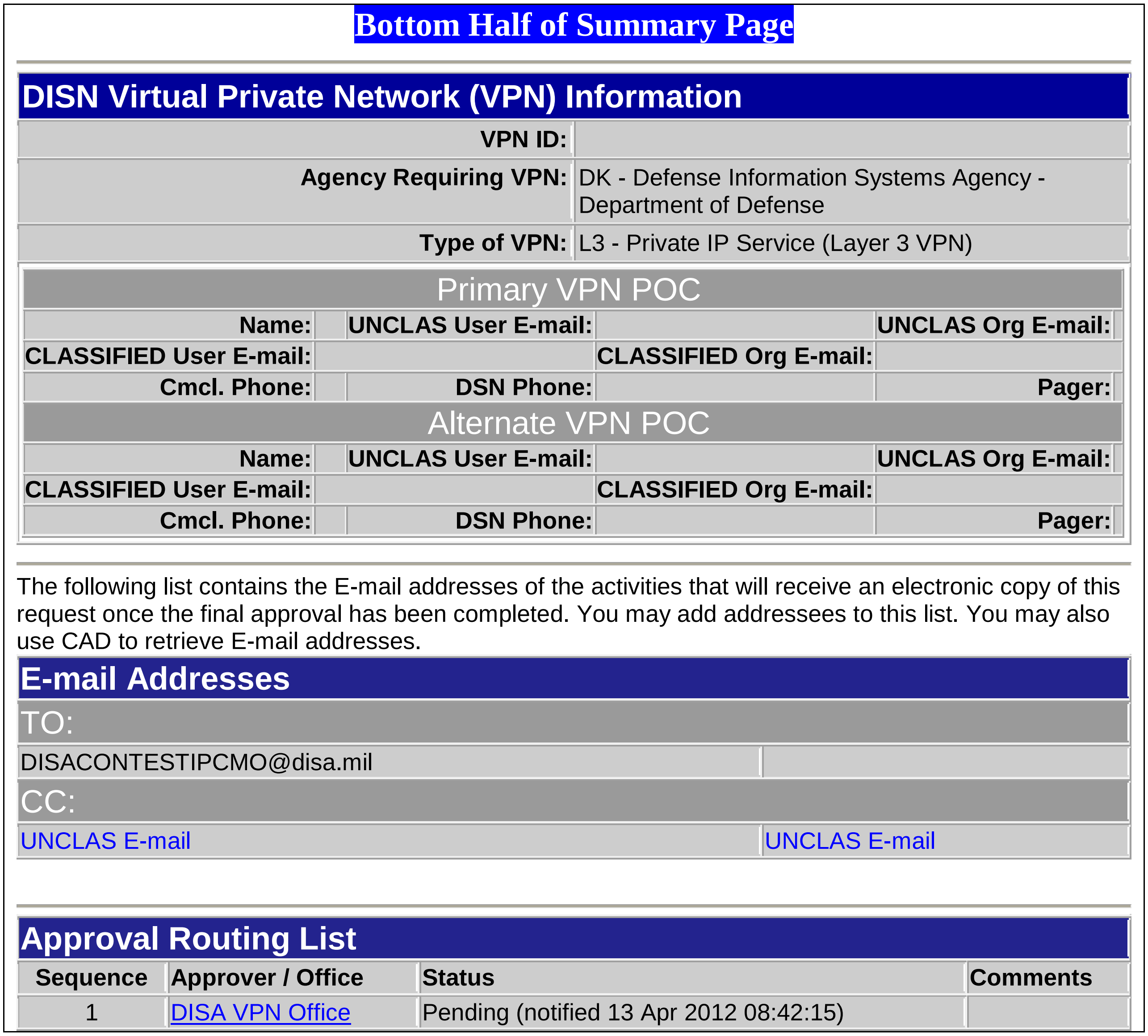
DISN Virtual Private Network (VPN) - Establish a VPN - Start

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:		**CLASSIFIED Org E-mail:**	
Cmcl. Phone:	phone number	**DSN Phone:**	

DISN Virtual Private Network (VPN) Details

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

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



Bottom Half of Summary Page

DISN Virtual Private Network (VPN) Information

VPN ID:	
Agency Requiring VPN:	DK - Defense Information Systems Agency - Department of Defense
Type of VPN:	L3 - Private IP Service (Layer 3 VPN)

Primary VPN POC					
Name:		UNCLAS User E-mail:		UNCLAS Org E-mail:	
CLASSIFIED User E-mail:		CLASSIFIED Org E-mail:			
Cmcl. Phone:		DSN Phone:		Pager:	

Alternate VPN POC					
Name:		UNCLAS User E-mail:		UNCLAS Org E-mail:	
CLASSIFIED User E-mail:		CLASSIFIED Org E-mail:			
Cmcl. Phone:		DSN Phone:		Pager:	

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:	
DISACONTESTIPCMO@disa.mil	
CC:	
UNCLAS E-mail	UNCLAS E-mail

Approval Routing List

Sequence	Approver / Office	Status	Comments
1	DISA VPN Office	Pending (notified 13 Apr 2012 08:42:15)	

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

Summary Page:

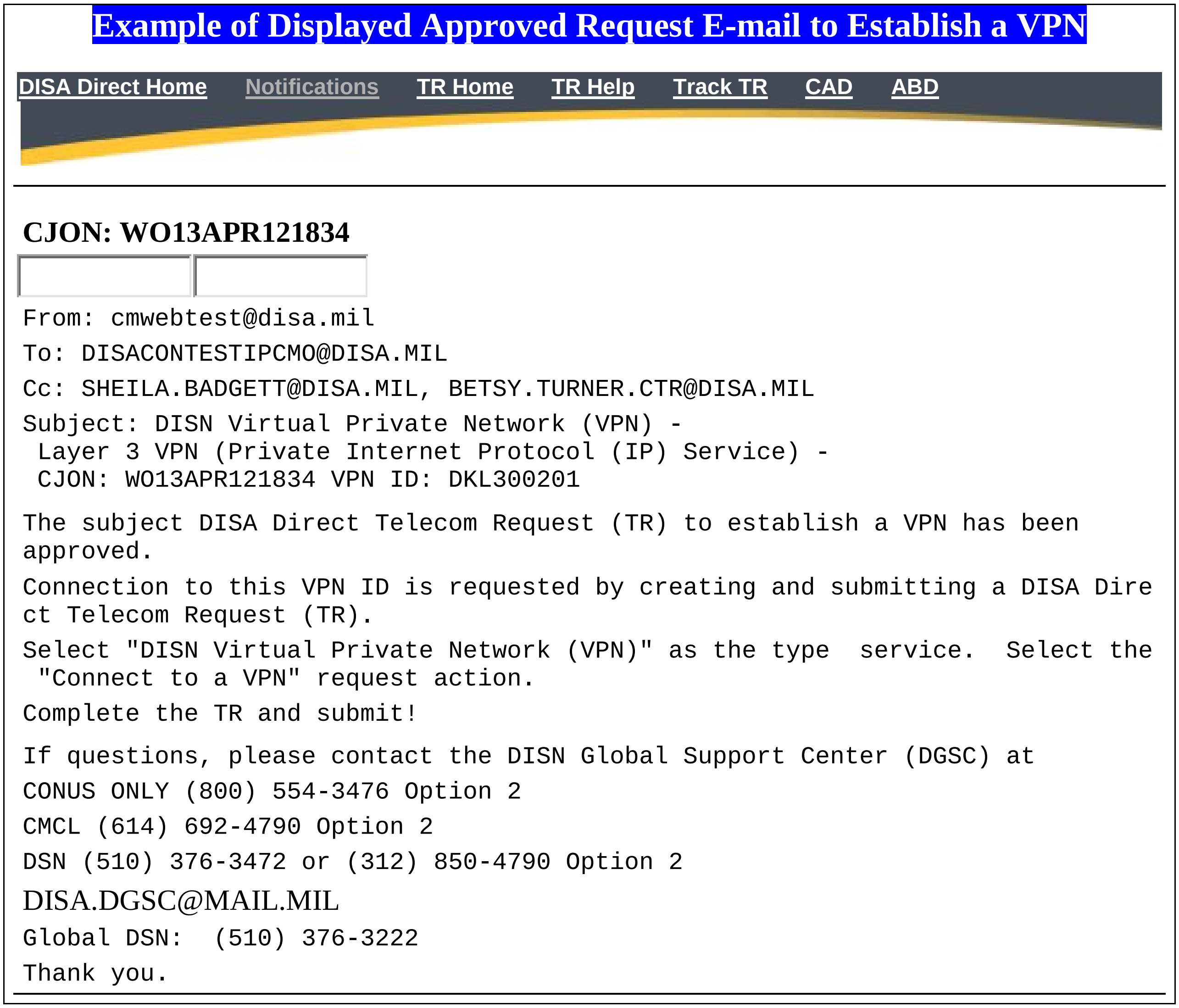
1. The user has three options on the Summary Page:

   a. **Delete Draft –** Allows the user to delete the requirement from the database.

   b. **Save as Draft –** Allows the user to save the information and return to complete later.

   c. **Submit Request –** Automatically changes the status of the TR to "Pending" and notifies the first routee in the VPN Routing List.

2. Upon final approval in the routing, an auto-generated e-mail will be sent to the engineering e-mail addresses based on the geographical disposition indicated in the TR. The e-mail also will be sent to all POCs and any additional e-mail addresses listed on the TR.



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

CJON: WO13APR121834

From: cmwebtest@disa.mil

To: DISACONTESTIPCMO@DISA.MIL

Cc: SHEILA.BADGETT@DISA.MIL, BETSY.TURNER.CTR@DISA.MIL

Subject: DISN Virtual Private Network (VPN) -
Layer 3 VPN (Private Internet Protocol (IP) Service) -
CJON: WO13APR121834 VPN ID: DKL300201

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

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

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

Complete the TR and submit!

If questions, please contact the DISN Global Support Center (DGSC) at

CONUS ONLY (800) 554-3476 Option 2

CMCL (614) 692-4790 Option 2

DSN (510) 376-3472 or (312) 850-4790 Option 2

DISA.DGSC@MAIL.MIL

Global DSN: (510) 376-3222

Thank you.

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

Other Informational Notes:

TR Homepage Options

1. **Copy Existing TR –** Does not apply to “Establish a VPN”; applies only to “Connect to a 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 a VPN.”

4. **Review Submitted TR –** Applies to both “Establish a VPN” and “Connect to a VPN.”

5. **Recall a TR –** Applies to both “Establish a VPN” and “Connect to a VPN.”

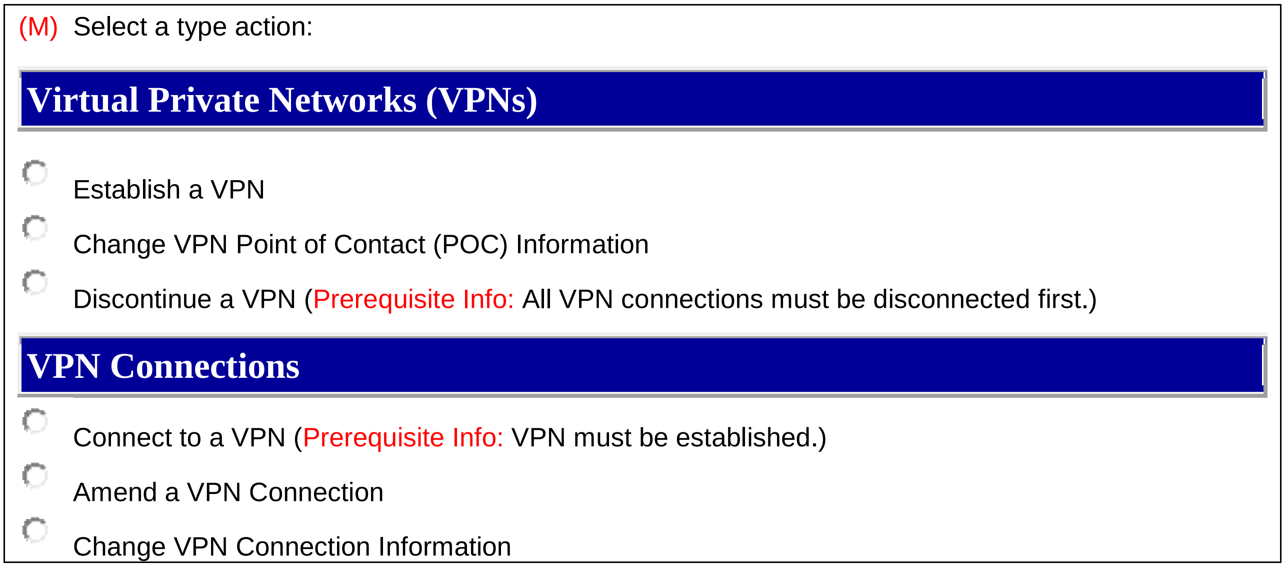
6. **Track TR –** Applies to both “Establish a VPN” and “Connect to a VPN.”

7.4 Other Action Requests – VPNs

Once the “Establish a VPN” request has been submitted, the other options may be used to “Change VPN Point of Contact (POC) Information” or “Discontinue a VPN.”

The “Change VPN Point of Contact (POC) Information” option may be used to change the Primary or Alternate POC information. When the request is submitted, it will route based on the VPN Routing ID identified on the TR. Upon final approval of the TR, an e-mail will be generated and sent to all e-mail addresses indicated on the TR Summary Page.

The “Discontinue a VPN” option is used to discontinue the use of the overall VPN. Before this action is taken, all of the VPN connections must be discontinued, and all actions completed. Actions in the “VPN Connections” section are addressed in Section 8, Connect to a VPN (Step 2).



(M) Select a type action:

Virtual Private Networks (VPNs)

○ Establish a VPN

○ Change VPN Point of Contact (POC) Information

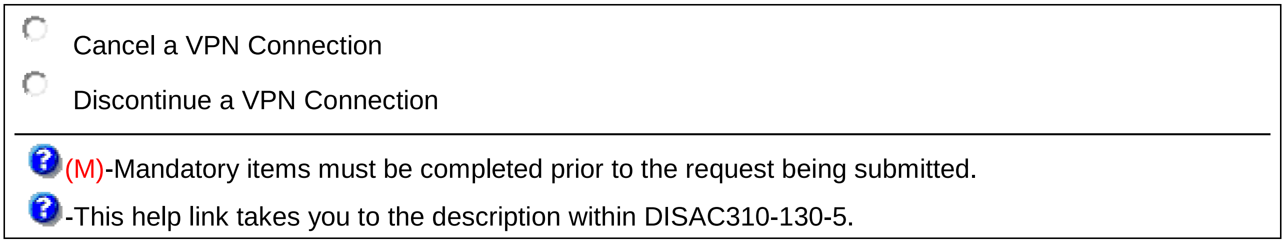
○ Discontinue a VPN (Prerequisite Info: All VPN connections must be disconnected first.)

VPN Connections

○ Connect to a VPN (Prerequisite Info: VPN must be established.)

○ Amend a VPN Connection

○ Change VPN Connection Information



○ Cancel a VPN Connection

○ Discontinue a VPN Connection

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

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

Figure 9: Request Action Page for Other Actions – VPNs

8. Connect to a VPN (Step 2)

8.1 Process Overview

The process to connect to a VPN, required for each location participating in the VPN, is similar to the existing process for ordering connections to SBU IP Data Service (formerly known as NIPRNet). This service option will result in generation of a TSR for each individual mission partner connection to the VPN; the TSR will be sent to the applicable DISA Provisioning Center. The basic procedures are as follows:

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 the 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 SBU IP Data Service ordering procedures.

5. In parallel, or shortly after initiating the request to connect to a VPN through DDOE, the mission partner should begin the Registration/Connection Approval Process as outlined in Appendix F of the DISN Connection Process Guide (CPG).

The following depicts the process overview for creating requests for individual mission partner connections to an established VPN. Business rules and specific steps are detailed in subsequent sections of this document.

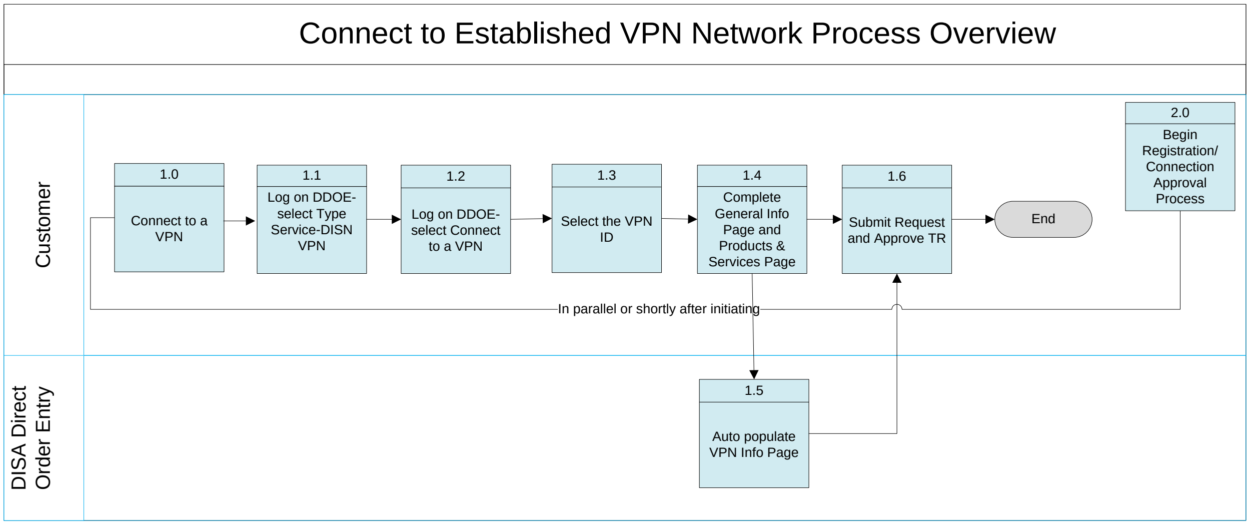

Connect to Established VPN Network Process Overview
Customer
DISA Direct Order Entry
1.0
Connect to a VPN
1.1
Log on DDOE-select Type Service-DISN VPN
1.2
Log on DDOE-select Connect to a VPN
1.3
Select the VPN ID
1.4
Complete General Info Page and Products & Services Page
1.6
Submit Request and Approve TR
End
2.0
Begin Registration/ Connection Approval Process
In parallel or shortly after initiating
1.5
Auto populate VPN Info Page

Figure 10: Process to Connect to a VPN

8.2 Business Rules

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

1. All DISA Direct users that have the role of ARO or DISA users that have the role of APO will have the capability to select DISN VPNs as the type of service.

2. The action types that apply to ***Connect to a 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 TR/TSR process. The SBU IP Data Service TR pages are the baseline used for the technical specifications for all "Connect to a VPN"-type actions.

   b. No funding is required, as this service falls within the DSS Cost Recovery Model. However, the service also will be accessible from non-DSS sites; the mission partner 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 of whether or not there is funding associated with the requirement.

   d. VPN Routing IDs, along with a VPN routing matrix or a PDC routing matrix, must have been established by the agency's RLO. These are available for selection when creating the TR. If unknown, a drop-down menu of RLOs is available.

3. Functionality in DDOE has 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 reconnection to the original VPN ID, a new request must be submitted. This request will require approval by the owner-agency.

4. Med COI for DMIX (Layer 3 VPN) users must use the DCN for this service: D314.

5. Private Data ISP Service only: Customers will be required to request IP address space from the DoD NIC for their connection to work in the Private Data ISP Service. Customers must obtain the IP address space out of the reserved IP space for Private Data ISP Service: 139.241.0.0/16.

   All customers requesting this service will be required to have DoD NIC assigned space from the following block of IPs: 139.241.0.0/16, 139.242.0.0/16, 139.243.0.0/16, 139.244.0.0/16, 139.245.0.0/16, 139.246.0.0/16, 139.247.0.0/16, 139.248.0.0/16. NOTE: Only 139.241.0.0/16 is currently open at the IAP. The other /16 blocks are reserved but not in use at this time.

   Additionally, all mission partners must include the following standard statement in the DoD NIC Template for IP Space:

   "This request is for Private Data ISP Service and requires IP space assignment from 139.241.0.0/16."

   Access https://www.nic.mil/ and complete the registration process to obtain the required IP address space. For issues with the registration process or the template, contact the DGSC (refer to Table 2). Select the "Network Information Center (NIC)" option.

   To obtain PTC approval from DISA for Private Data ISP Service, the mission partner must submit an ATO from their DAA containing the following statement:

   No ingress or egress restrictions are provided by DISA. DAA understands that this service has no Computer Network Defense (CND) or firewall protections, and the DAA is assuming the risk associated with an open Internet connection.

   The ATO also must include:

   a. The CCSDs of the two virtual circuits must be in the subject line of the ATO.

   b. The IP address space assigned by the DoD NIC must be included in the ATO.

6. QoS Implemented – QoS is the ability to provide different priorities to different pre-marked packets (applications, users, or data flows) or to guarantee a certain level of performance to those packets across the DISN. It does not give one mission partner's traffic a higher priority than another mission partner's traffic.

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

Effective immediately, the TR will auto-populate the type of QoS template. The following types of service offerings will reflect QoS GTP: DISN VPN (Private IP Service (Layer 3 VPN)) - L3, Private LAN Service (Layer 2 VPN) - L2, and Label Transport Service (Layer 2 CsC) - CX. The QoS template code will be reflected automatically in TSR Item 142. Service offerings not listed here, will not reflect QoS.

7. The CJCSI 6211.02D, Enclosure D, paragraph 15, states that DSAWG approval must be obtained "before tunneling classified data across unclassified IP infrastructure." DSAWG has granted DISA approval authority for tunneling classified traffic over unclassified MPLS routers if the following conditions are met.
    a. The DAA ATO letter must have the following statement:

       The DAA understands that classified information sent to DISA will be Type 1 or Suite B cryptography encrypted prior to transmission and traffic is routed by the DISN unclassified router network.
    b. Connection will be on a dedicated physical interface on the DISN unclassified router. NOTE: Virtual interfaces will be permitted when testing has been completed and Configuration Control Board (CCB) approval has been granted (expected in March or April 2015).
    c. There are no backdoor connections (NIPRNet, SIPRNet, etc.).
    d. The standard QoS 6 queue model is applicable.
    e. Detailed topology showing all connections is required.

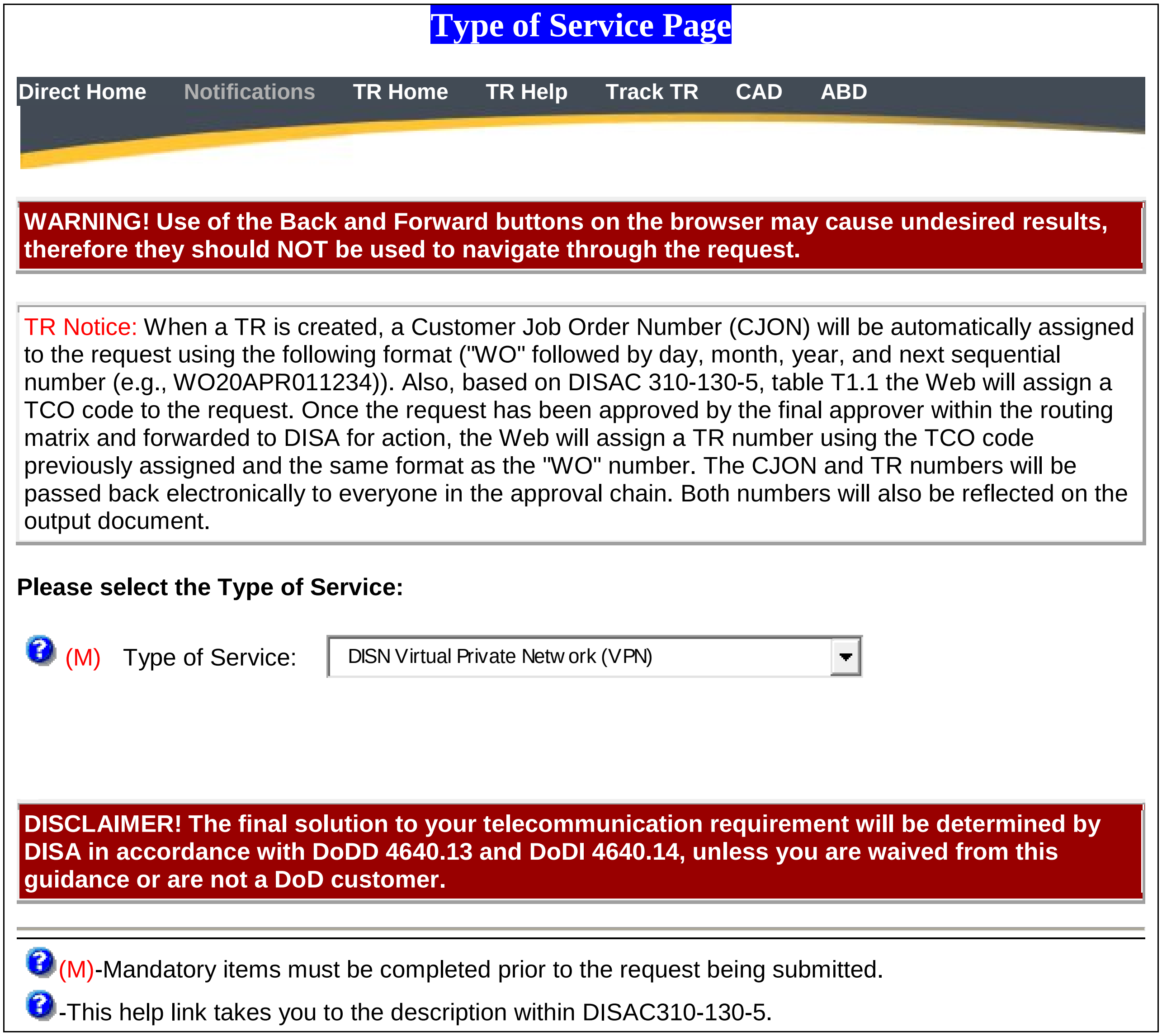
   Any connections that do not meet the above requirements must have DSAWG approval prior to being granted PTC to the DISN.

8.3 Steps to Connect to a VPN on DDOE

This section details the steps for requesting individual physical VPN connections to an established VPN (network). ***NOTE: The VPN must be established prior to requesting physical connections.*** Table 1 identifies specific VPN types that are DISA-established VPNs. Mission partners cannot establish these VPN types; they can only request connections to them.

All steps and screens to Connect to a VPN are the same for all VPN service types (L2, L3, CX, and TE). The examples provided are specifically for 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

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) ▼

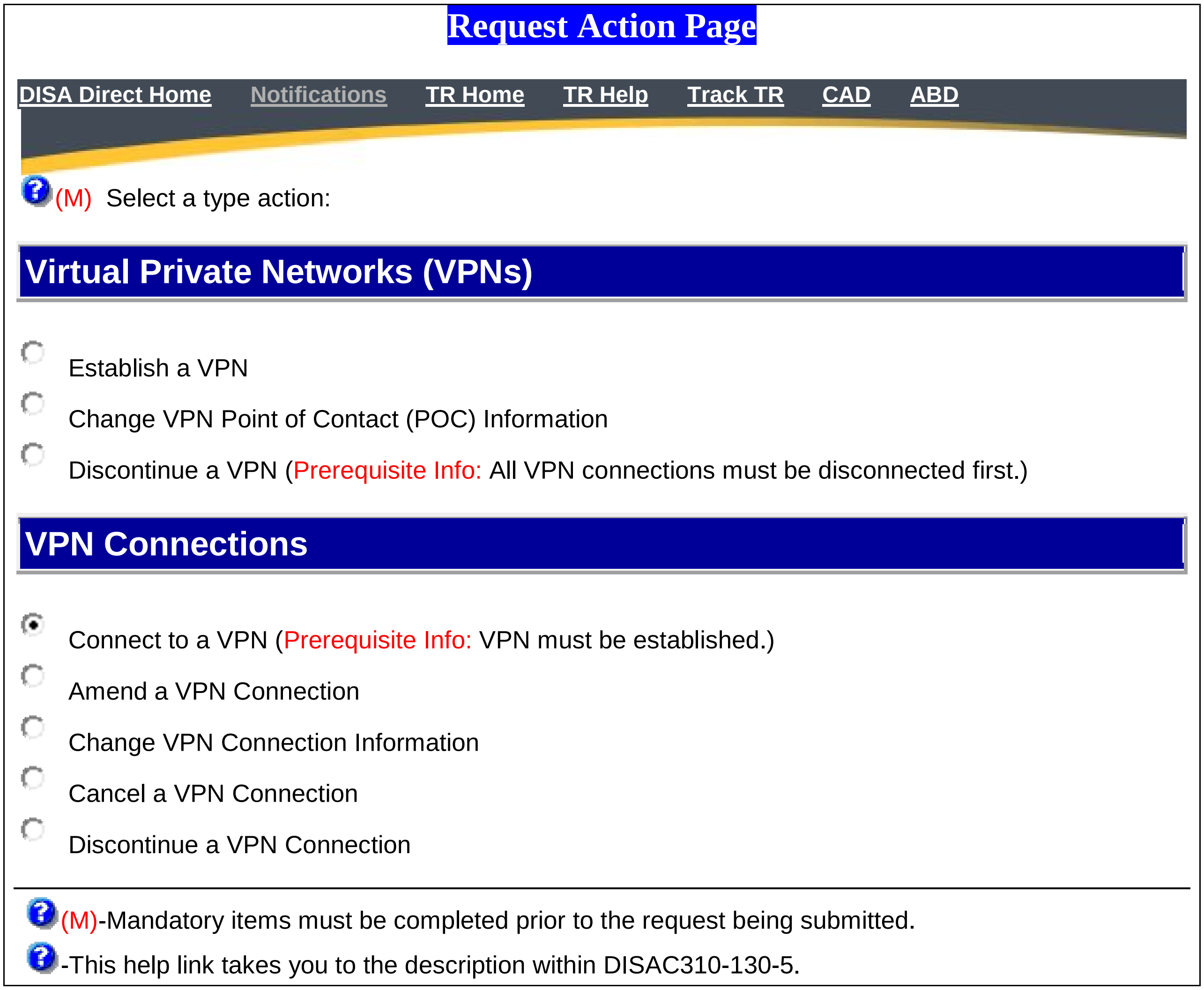
DISCLAIMER! The final solution to your telecommunication requirement will be determined by DISA in accordance with DoDD 4640.13 and DoDI 4640.14, unless you are waived from this guidance or are not a DoD customer.

?(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 11: 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

(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.

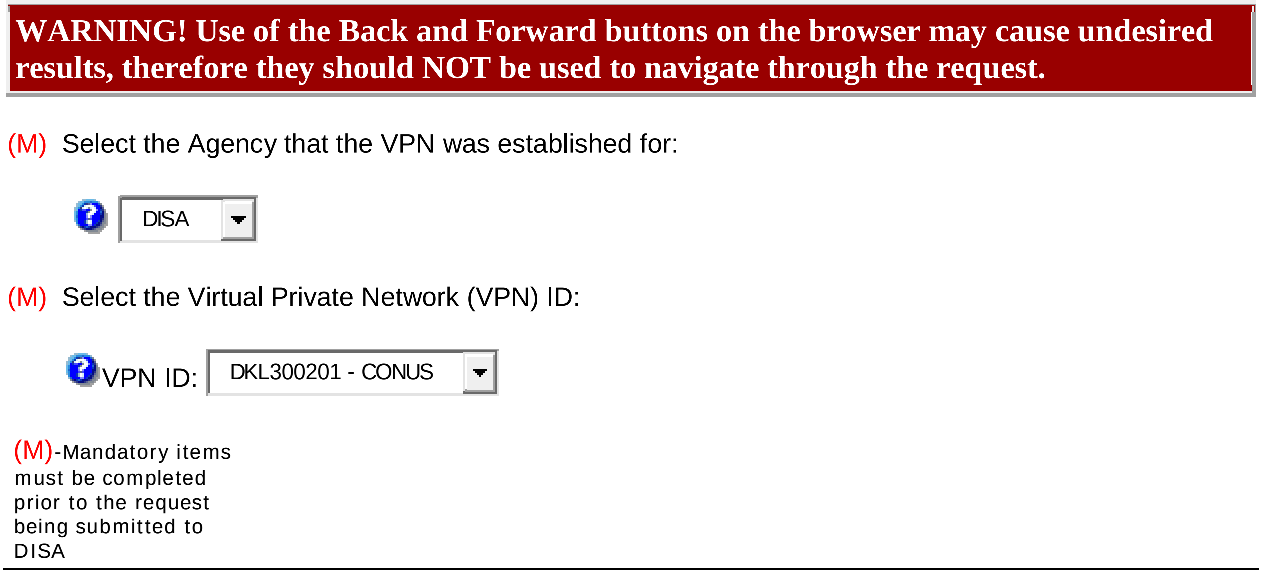
-This help link takes you to the description within DISAC310-130-5.

Figure 12: Request Action Page

ACTION: The Search Page presented will vary depending on the role of the user logged into DDOE; the page will include all VPN IDs of established VPNs created for the user. The user selects the applicable VPN ID from the drop-down menu for the established L2, L3, TE, and 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 for 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

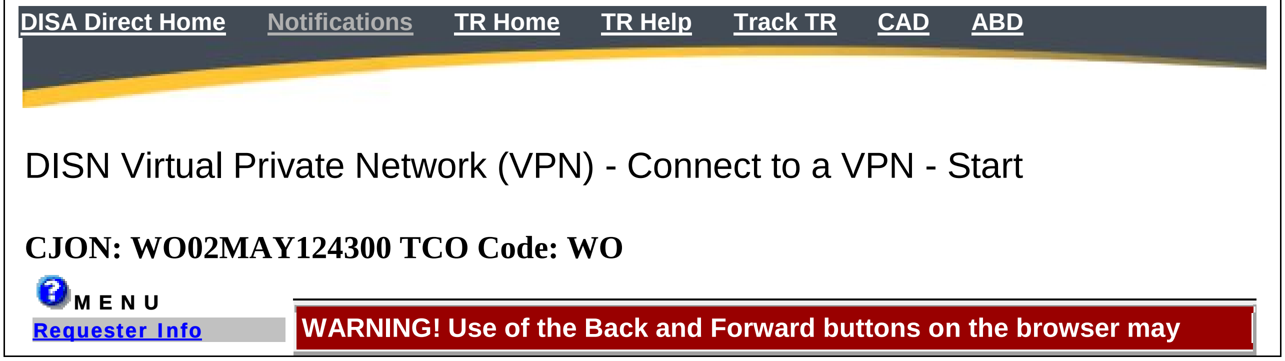
(M)-Mandatory items must be completed prior to the request being submitted to DISA

Figure 13: Example of Search Page

The 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.

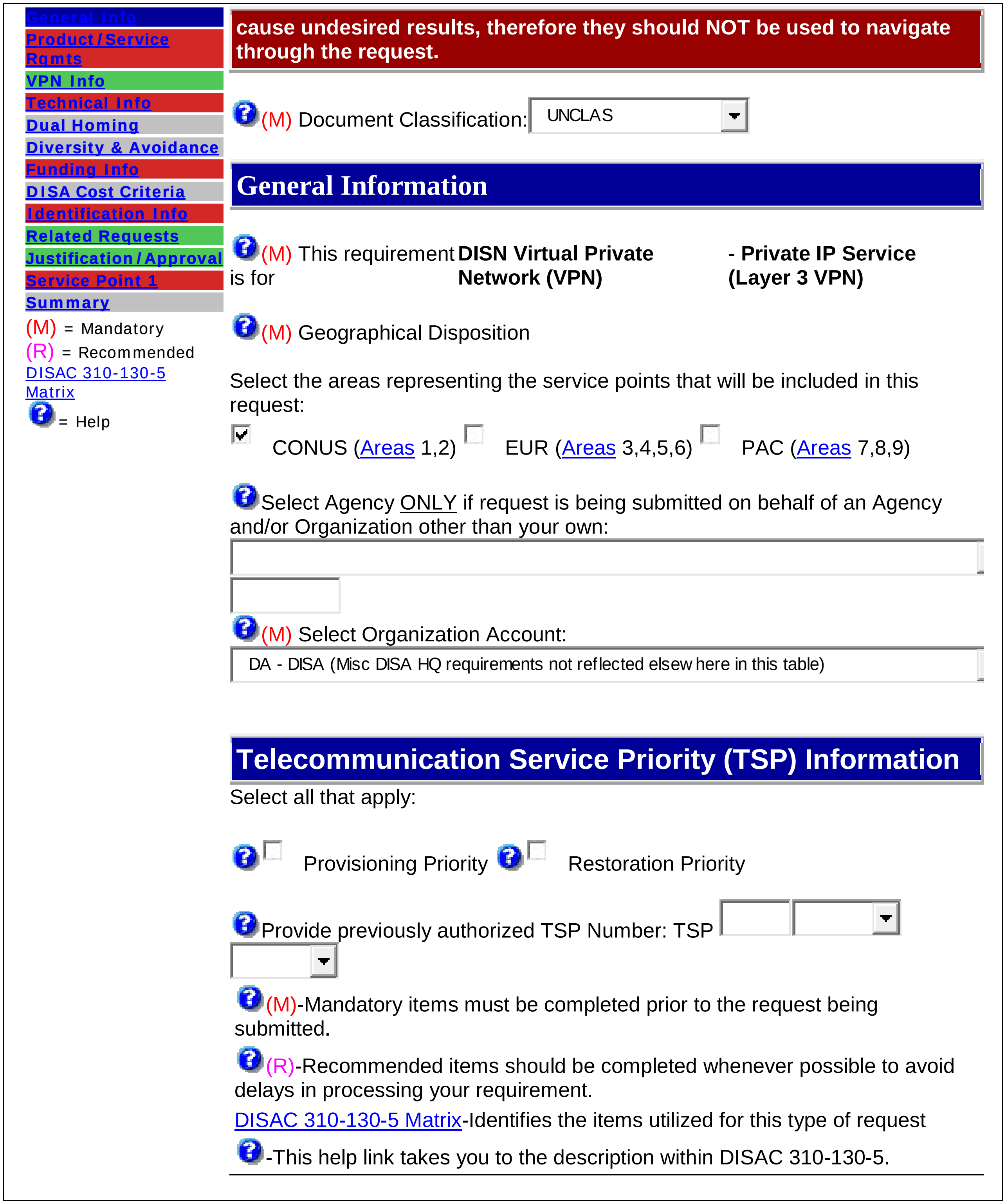
General Information Page



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

CJON: WO02MAY124300 TCO Code: WO

WARNING! Use of the Back and Forward buttons on the browser may



(M) = Mandatory
(R) = Recommended
DISAC 310-130-5 Matrix
? = Help

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 14: General Information Page

General Information Page:

1. **General Information** – This section automatically displays the service type 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 1) Private Data ISP Service, VPN ID: *DKL300227*, 2) IAP DMZ, VPN ID: *DOL300230*, 3) CMNT COI Layer 3, VPN ID: *DKL342000*, 4) Med COI Layer 3, VPN ID: *DKL300251*, and 5) MPG COI, VPN ID: *DKL300249*, the Private IP Service (Layer 3 VPN) will be displayed.

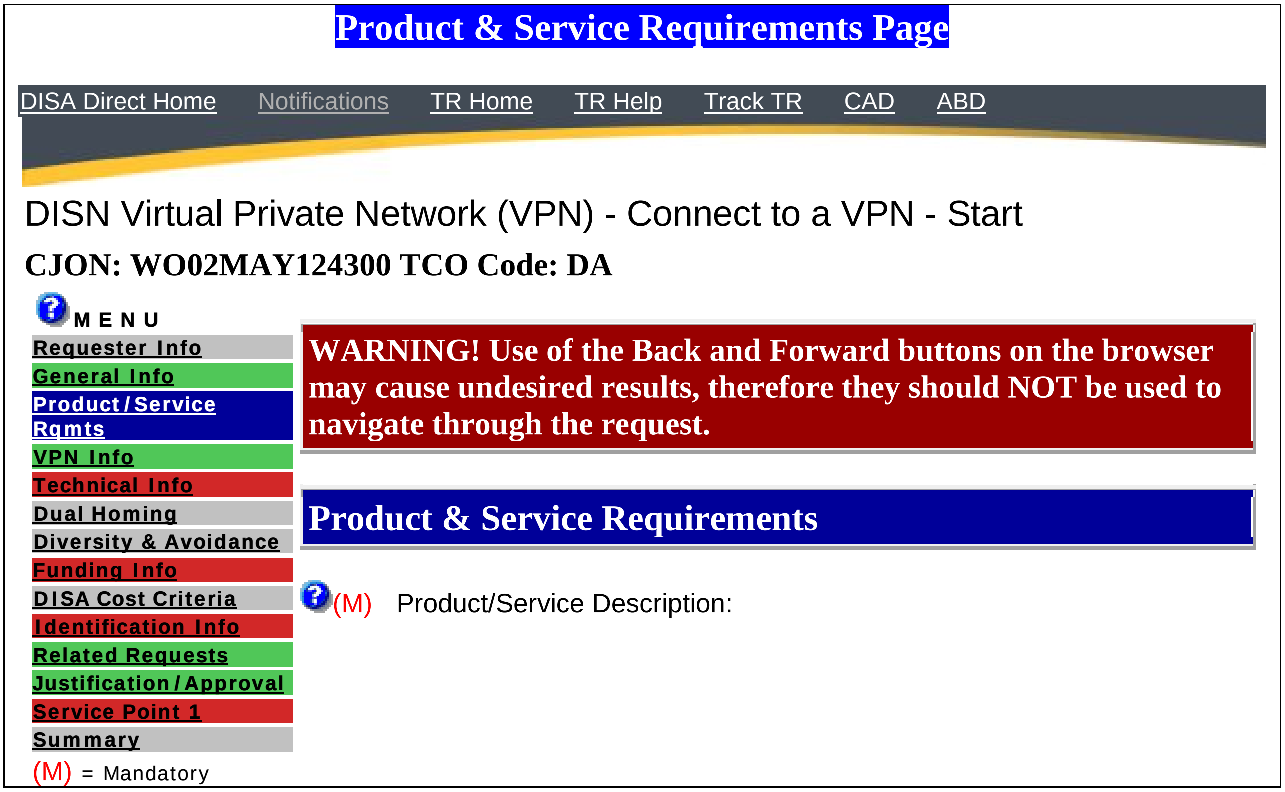
   a. **Geographical Disposition** – This mandatory selection indicates the area that the service points will represent.

   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 whether the connection is being written on behalf of another agency.

   c. **Select Organization Account** – This mandatory selection is presented when applicable for the Telecommunications Certification Office (TCO) code.

2. **Telecommunication Service Priority (TSP) Information** – This section is optional, but must be completed if TSP is required.

ACTION: The 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

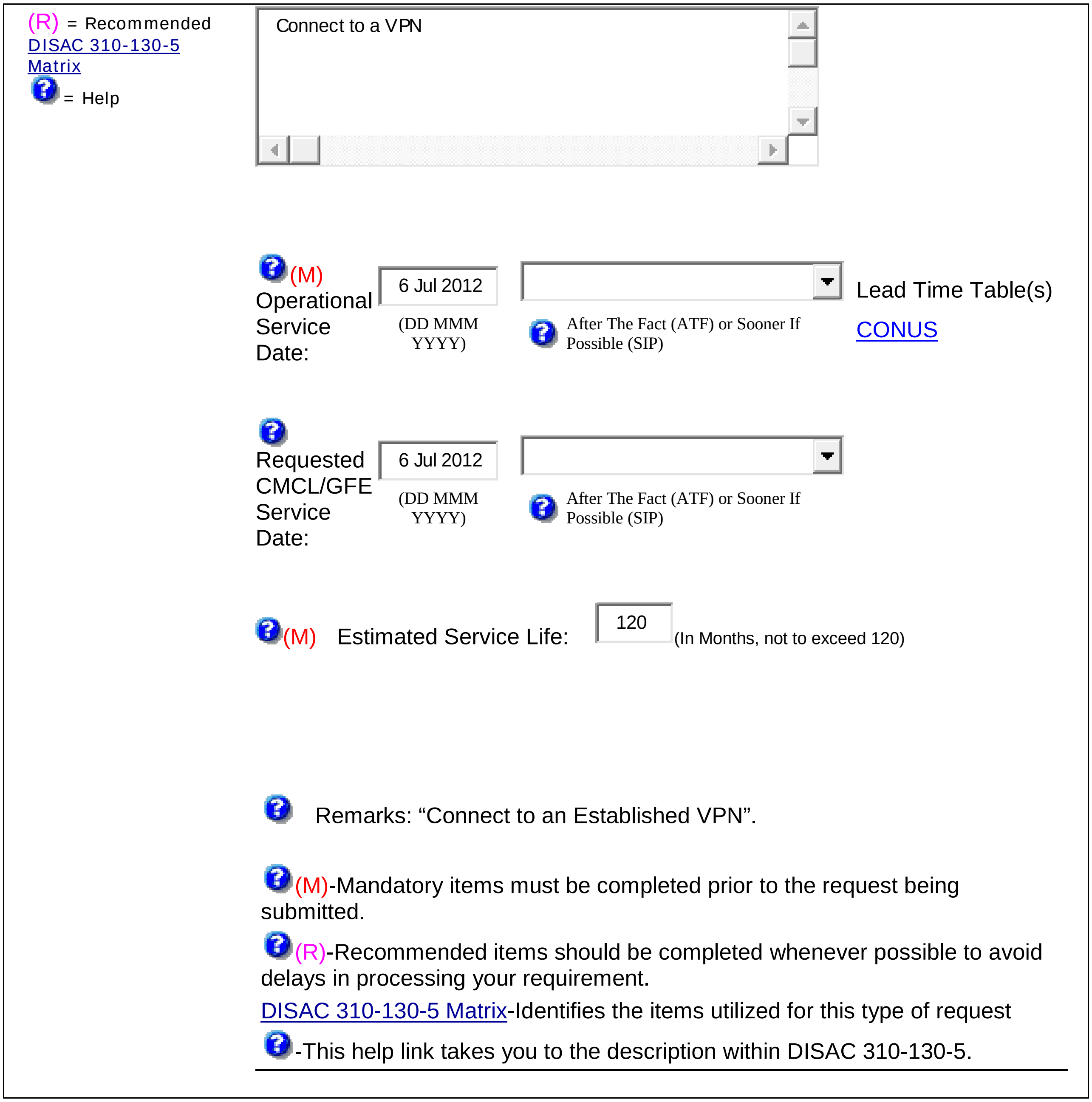
DISN Virtual Private Network (VPN) - Connect to a VPN - Start

CJON: WO02MAY124300 TCO Code: DA

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:



(R) = Recommended
DISAC 310-130-5 Matrix
❓ = Help

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)

❓ Remarks: “Connect to an Established VPN”.

❓(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 15: 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 of action selected by the ARO/APO: "Connect to a VPN." The user may modify or insert additional information.

   b. **Operational Service Date** – This mandatory field indicates the operational service date.

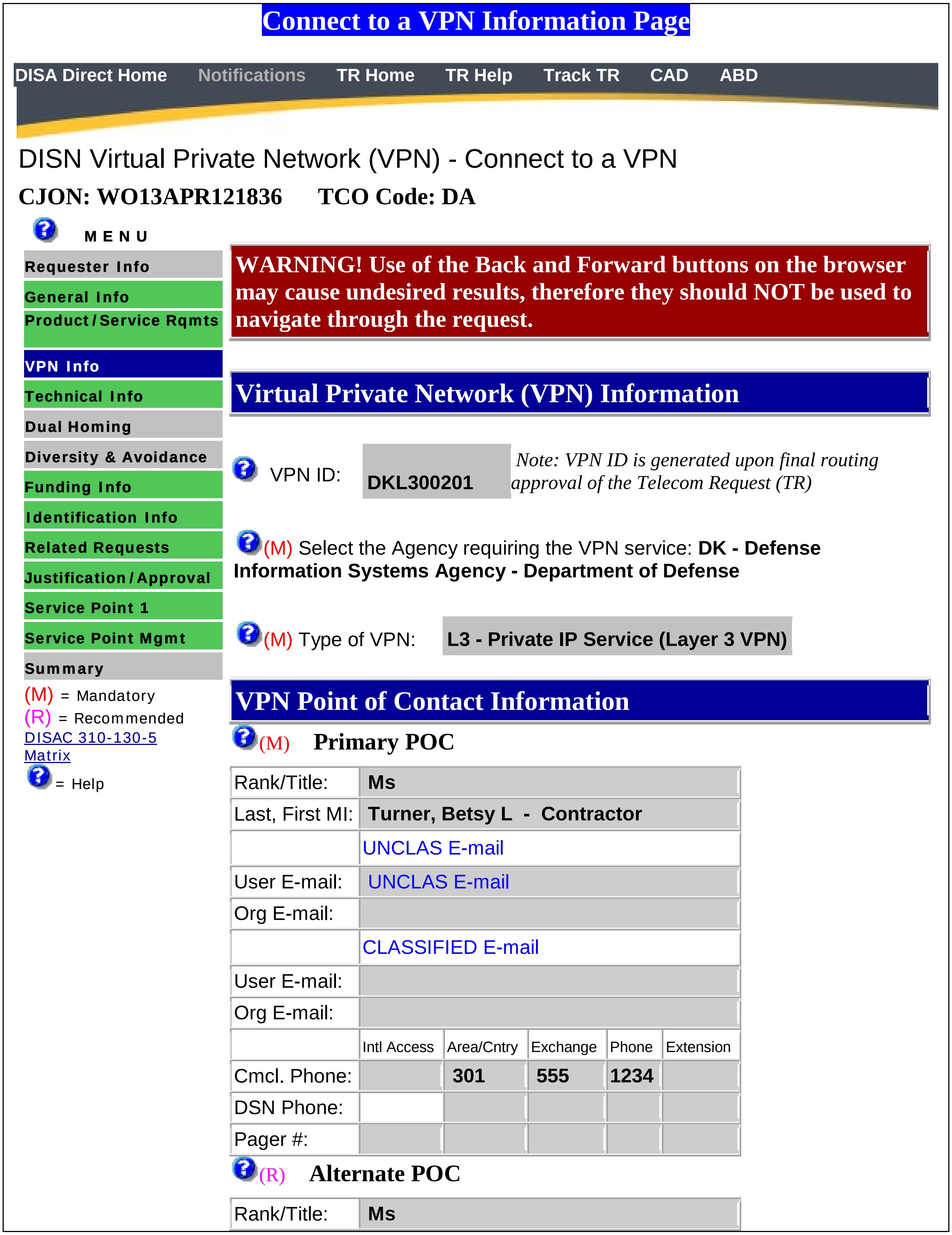
   c. **Requested CMCL/GFE Service Date** – This mandatory field indicates the requested service date.

   d. **Estimated Service Life** – This recommended field to indicate the length of time for the connection.

   e. **Remarks** – Mission partners should input "Connect to an Established VPN" for all VPN types.

ACTION: The Connect to a VPN Information Page is presented as shown in the following figure. The page is auto-populated with 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.

Figure on next pages



Connect to a VPN Information Page

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

CJON: WO13APR121836 TCO Code: DA

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)**

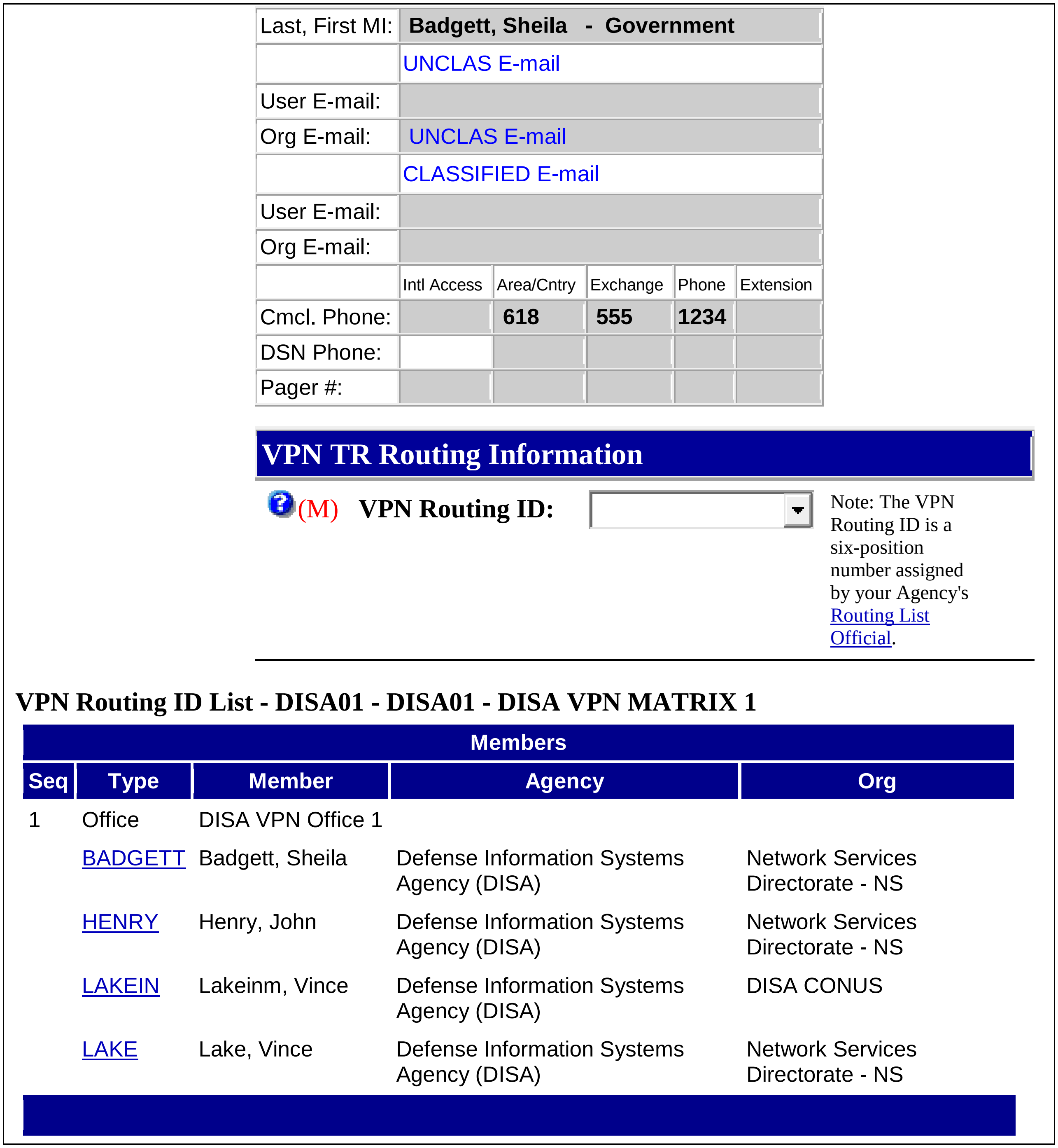
VPN Point of Contact Information

(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:** ▼

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 16: Connect to a VPN Information Page

<u>Connect to a VPN Information Page</u>:

3. **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 codes of the VPN ID, along with the description based on DISAC 310-65-1, Chapter 3, “Agency Requiring the Service,” paragraph 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 be displayed automatically; for example, L2, L3, CX, or TE. There are currently five exceptions; when connecting to 1) Private Data ISP Service, VPN ID: *DKL300227*, 2) IAP DMZ, VPN ID: *DOL300230*, 3) CMNT COI Layer 3, VPN ID: *DKL342000*, 4) Med COI Layer 3, VPN ID: *DKL300251*, and 5) MPG COI, VPN ID: *DKL300249*, the Private IP Service (Layer 3 VPN) will be displayed. *NOTE: The example shown is for a “L3 - Private IP Service (Layer 3 VPN).”*

4. **VPN Point of Contact Information –** This section provides the primary and alternate POC information for the VPN.

5. **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 exceptions are the DISA-established VPN types listed in Table 1. All DISA-established VPNs will route automatically route to DISA for approval.

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

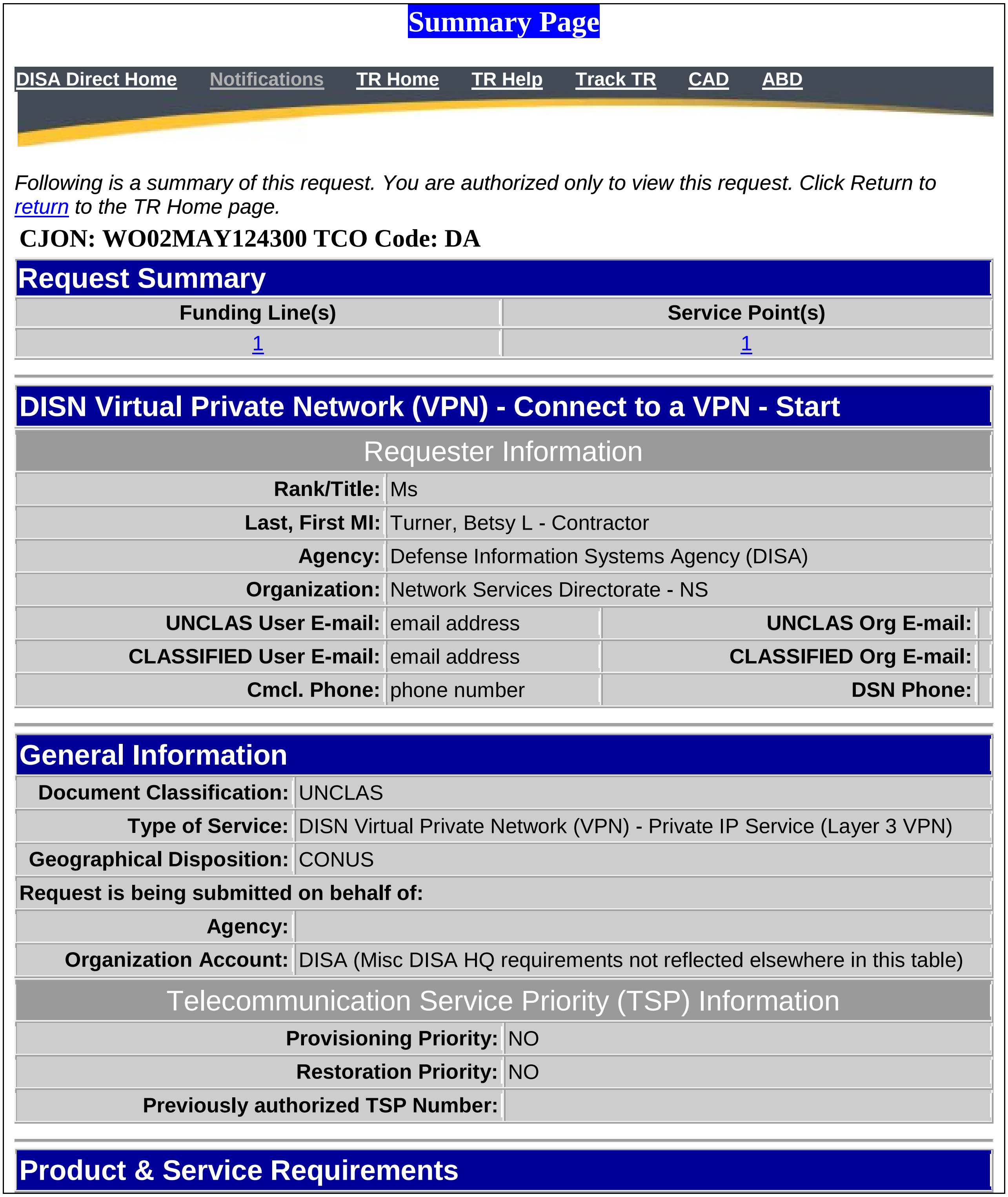
Identification Information Page:

Complete information for your CCSD.

1. **Purpose/Use –** “PN” will be populated automatically by DDOE as the Purpose/Use code. “PN” is used for all VPNs.

2. **Type of Service –** The user must select “G - Permanent Virtual Circuits” as the Type of Service entry.

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 of a TR to connect to a VPN.



Summary Page

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:**	

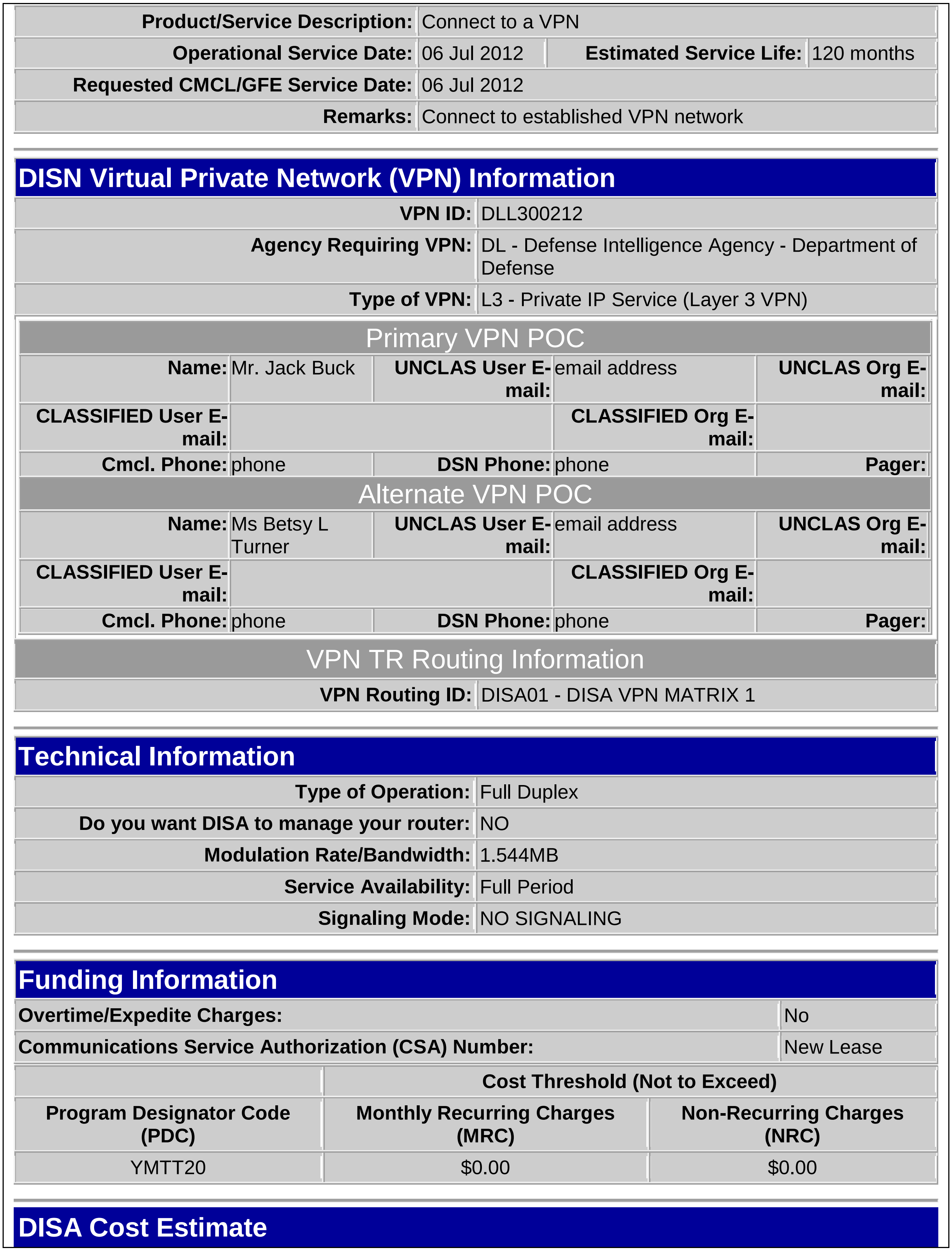
General Information

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

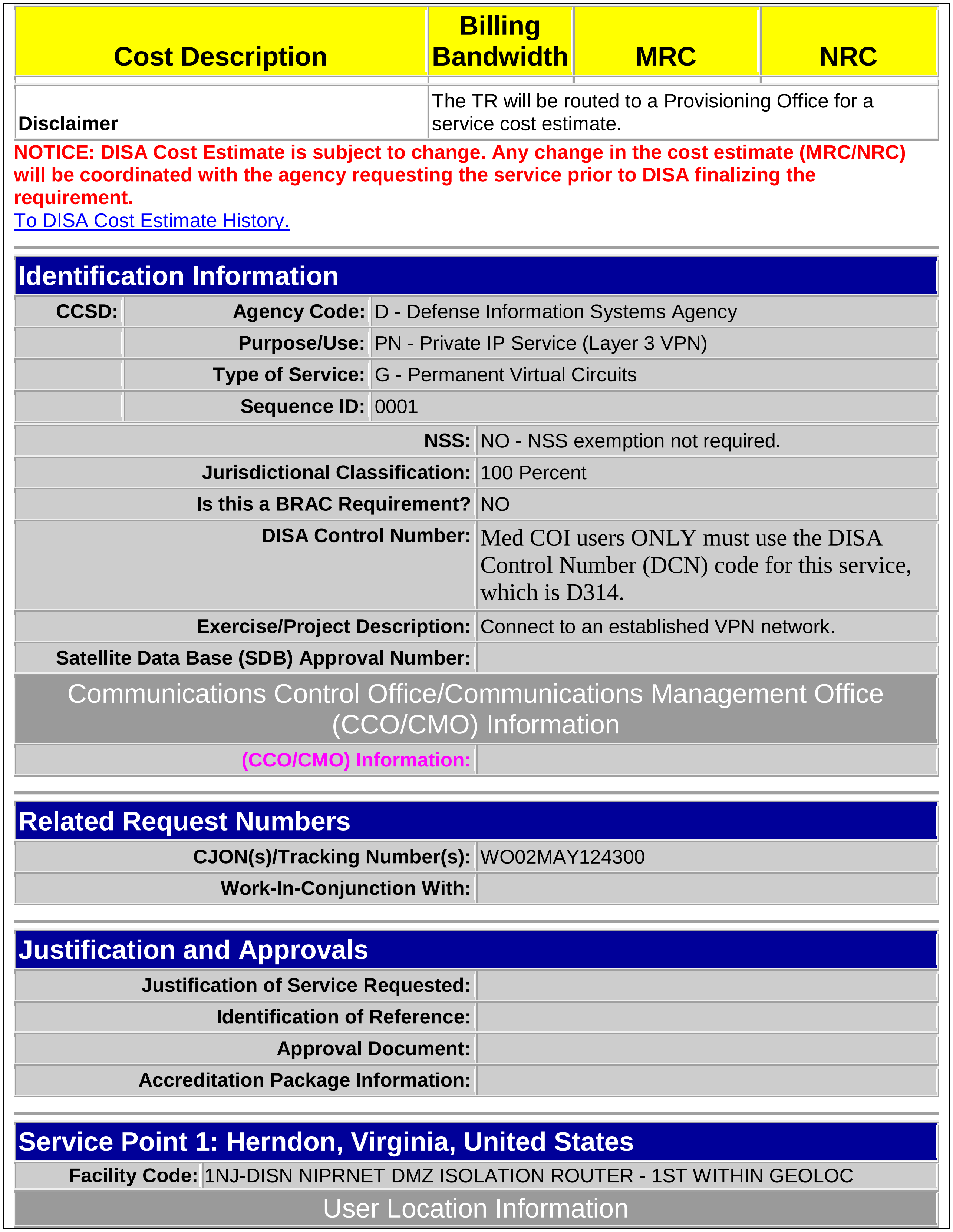
Type of Operation:	Full Duplex
Do you want DISA to manage your router:	NO
Modulation Rate/Bandwidth:	1.544MB
Service Availability:	Full Period
Signaling Mode:	NO SIGNALING

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:	Med COI users ONLY must use the DISA Control Number (DCN) code for this service, which is D314.
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:	

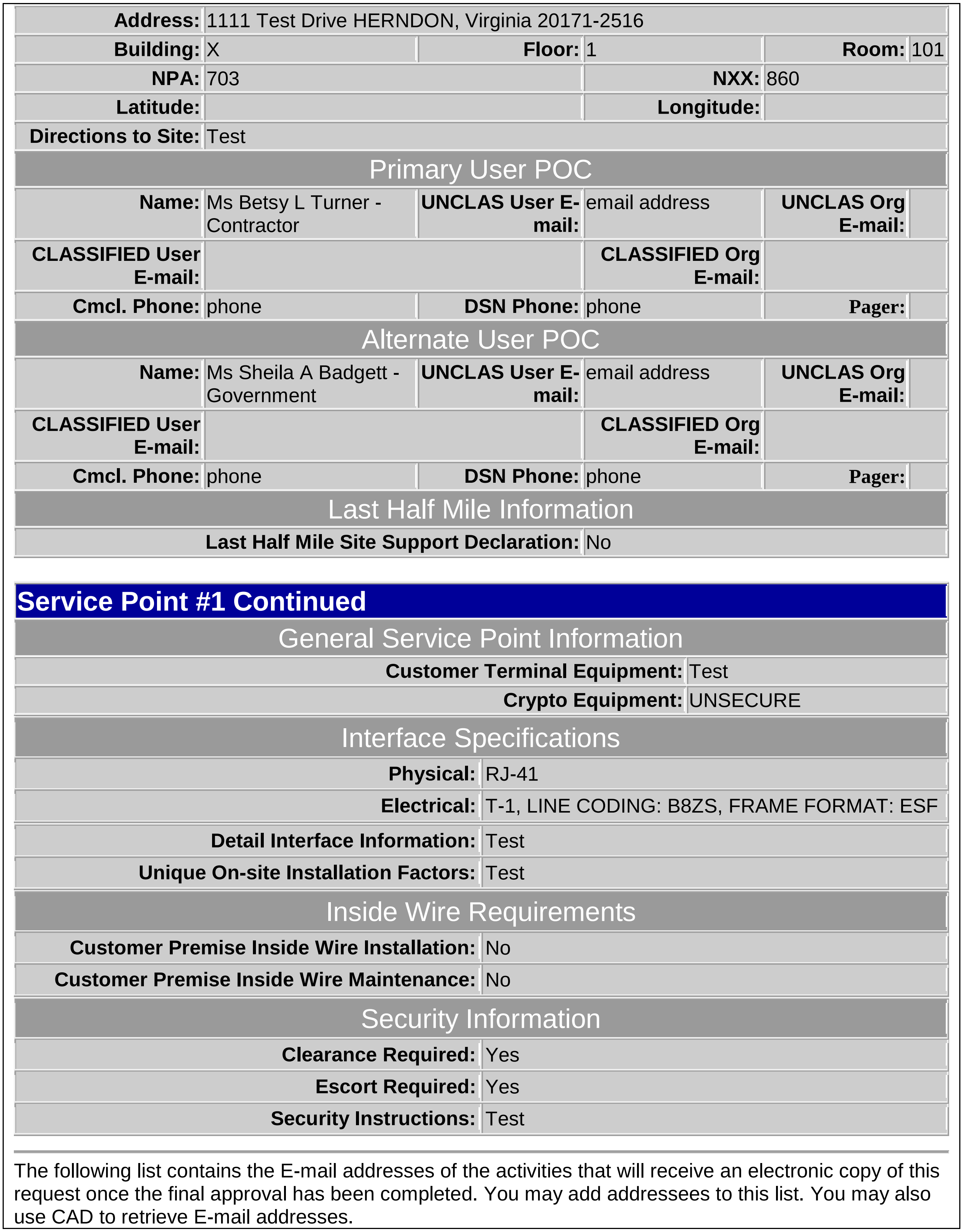
Justification and Approvals

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

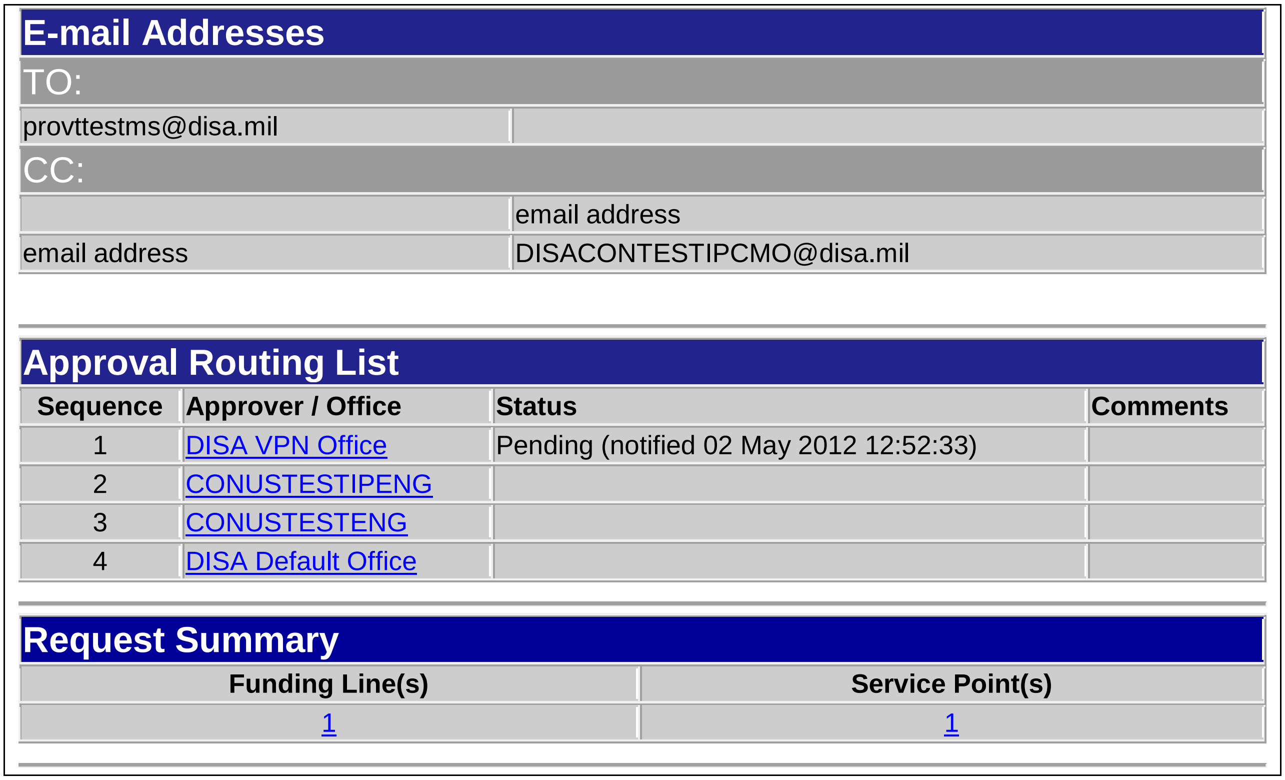
Inside Wire Requirements

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 17: 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 18: Example of TSR to Connect to an L3 VPN

<u>Other Informational Notes:</u>

TR Homepage Options

1. **Copy Existing TR –** Applies only to “Connect to a VPN.”

2. **Import a TSR –** Does not apply to any VPN services.

3. **Retrieve a Draft TR –** Applies to both “Establish a VPN” and “Connect to a VPN.”

4. **Review Submitted TR –** Applies to both “Establish a VPN” and “Connect to a VPN.”

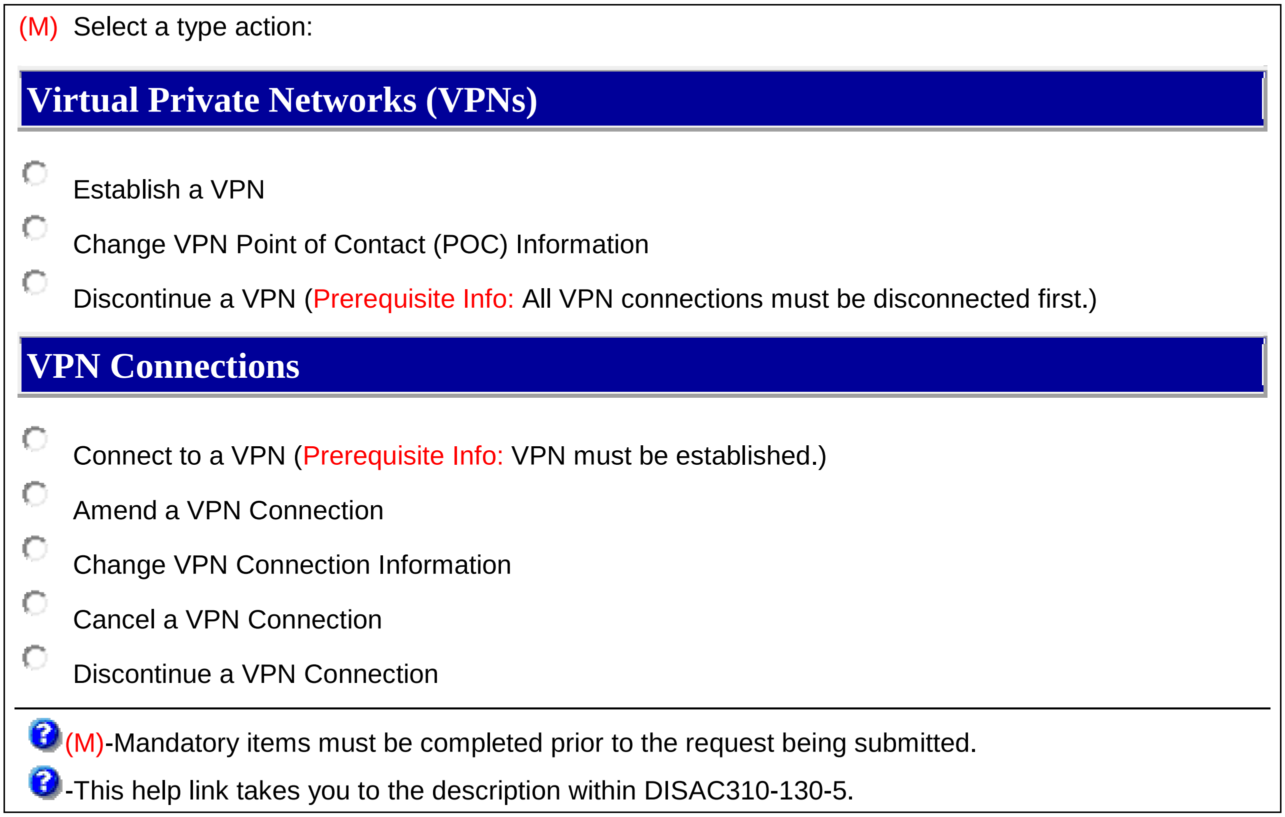
5. **Recall a TR –** Applies to both “Establish a VPN” and “Connect to a VPN.”

6. **Track TR –** Applies to both “Establish a VPN” and “Connect to a VPN.”

8.4 Other Action Requests – VPN Connections

Users will note that the request for these services is based on the same type of actions as those for 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,” “Cancel a VPN Connection,” or “Discontinue a VPN.” 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 "Connect to a VPN" request 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 is still in the ordering process, select the "Cancel a VPN Connection" option. The "Virtual Private Networks (VPNs)" section actions are addressed in Section 7, Establish a VPN (Step 1).



(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 19: Request Action Page for Other Actions – VPN Connections

Note that 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 the established VPN must be disconnected and/or canceled before the VPN can be discontinued***. Information on discontinuing an established VPN is provided in Section 7.4, Other Action Requests – VPNs.

Appendix A
Acronym List

Acronym	Term
APO	Authorized Provisioning Official
AR	Aggregation Router
ARO	Authorized Requesting Official
ATM	Asynchronous Transfer Mode
ATO	Authority to Operate
BGP	Border Gateway Protocol
BRM	Business Relationship Management
BSC	Business Service Catalog
CAD	Central Address Directory
CAP	Connection Approval Process
CC/S/A/FA	Combatant Command, Service, Agency, or Field Activity
CCB	Configuration Control Board
CCSD	Command Communications Service Designator
CE	Customer Edge
CENTRIXS	Combined Enterprise Regional Information Exchange System
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJON	Customer Job Order Number
CMNT	Coalition Mission Network Transport
CND	Computer Network Defense
CNDSP	Computer Network Defense Service Provider
COCOM	Combatant Command
COI	Community of Interest
COMSEC	Communications Security
CPG	Connection Process Guide
CsC	Carrier Supporting Carrier
CY	Calendar year
DAA	Designated Approving Authority
DCN	DISA Control Number
DDOE	DISA Direct Order Entry
DECC	Defense Enterprise Computing Center
DGSC	DISN Global Support Center
DISA	Defense Information Systems Agency
DISAC	DISA Circular
DISN	Defense Information Systems Network

Acronym	Term
DMIX	Defense Medical Information Exchange
DMZ	Demilitarized Zone
DoD	Department of Defense
DoDI	DoD Instruction
DSAWG	Defense IA Security Accreditation Working Group
DSS	DISN Subscription Service
DTEN	DISN T&E Network
DTES	DISN Test and Evaluation Service
eBGP	External Border Gateway Protocol
FY	Fiscal year
GIAP	Global Information Grid Interconnection Approval Process *Now also known as Department of Defense Information Networks (DoDIN) Interconnection Approval Process*
GIG	Global Information Grid *Now also known as Department of Defense Information Networks (DoDIN)*
GTP	General Transport Path
IA	Information Assurance
IAP	Internet Access Point
IAPNet	IAP Network
iEHR	Integrated Electronic Health Record
IP	Internet Protocol
IPT-PE	IP Transport-Provider Edge
ISP	Internet Service Provider
JB-CE	Joint Base-Customer Edge
JIE	Joint Information Environment
JR-CE	Joint Router-Customer Edge
JRSS	Joint Regional Security Stack
LAN	Local Area Network
LSTDM	Low-Speed Time Division Multiplexing
Med COI	Medical Community of Interest
MPG	Mission Partner Gateway
MPLS	Multiprotocol Label Switching
NFE	NIPRNet Federated Gateway External
NFG	NIPRNet Federated Gateway
NIC	Network Information Center
NIPRNet	Sensitive but Unclassified IP Router Network
NS	Network Services Directorate
NSC	NS Enterprise Connection Division
PDC	Program Designator Code

Acronym	Term
POC	Point of Contact
PTC	Permission to Connect
QoS	Quality of Service
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
T&E	Test and Evaluation
TCO	Telecommunications Certification Office
TR	Telecommunications Request
TSO	Telecommunications Service Order
TSP	Telecommunication Service Priority
TSR	Telecommunications Service Request
UPE	Unclassified Provider Edge
VA	Department of Veterans Affairs
VPN	Virtual Private Network
VPN ID	VPN Identifier
VRF	Virtual Routing and Forwarding

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