SECRET IP DATA

Sign up to receive Secret IP Data email updates

SERVICE SUPPORT

DISN Global Support Center DSN: (510) 376-3222 or (312) 850-4790 CML: (800) 554-3476 or (614) 692-4790 DGSC@CSD.DISA.MIL DGSC@COLS.CSD.DISA.SMIL.MIL

HOW TO ORDER

Services can be ordered using the DDOE application located on DISA Direct

DESCRIPTION

The Secret IP Data provides service that provides point-to-point connectivity to customers. It also provides access to secret data, e-mail, and web services content.

The Secret IP Data provides IP-based secret information transfer across DoD for official DoD business applications such as e-mail, web services, and file transfer. The Secret IP Data service gateway function provides DoD customers with centralized and protected connectivity to federal, Intelligence Community (IC), and allied information at the secret level. The Secret IP Data service includes IP-based secret information exchange within DoD (DoD intranet) and centralized, gateway external network information exchange (i.e., the extranet). The intranet function provides access to a joint, shared DoD environment at the secret classification level for the exchange of information among DoD components.

This service requires customer provided encryption devices. For more information, please reference the Secret IP Router Network (SIPRNet) Customer Guide 10-December-2009.

FEATURES

Connectivity Features

- Classification Segmentation—Joint, DoD-wide enterprise internetworking enables the exchange of secret information.
- Rate-Limited Access Bandwidth—IP data rate limited to the customer-requested access bandwidth up to the maximum supported by the interface.
- Control and Routing Exchange—Static configuration or dynamic updates using the Border Gateway Protocol (BGP) that are supported for IP routing between the DISN edge and Customer Edge (CE) routers.
- Dial-Up Access—Remote workstation access to the Secret IP Data service through the Public Switched Telephone Network (PSTN) or Integrated Services Digital Network (ISDN) and Secure Telephone Unit or Secure Terminal Equipment (STE).

Information Assurance Protection Features

- Access Load-Sharing and Diversity—This feature supports multiple access links to improve service survivability. Options for ordering access circuits include loadsharing (active/active) and primary with secondary backup (active/standby) for interface, node, or site diversity to meet site C2 survivability requirements.
- External Network Gateways for Perimeter Protection—This feature provides protected, centralized interfaces to external networks. The classified federal demilitarized zone (DMZ) and releasable DMZ provide secure connectivity to the IC and other federal government and allied networks operating at the secret level.

Network Management Features

- Configurable Aggregate Access Bandwidth—The service access bandwidth will be configurable up to the maximum supported by the access physical interface through the service portal.
- Configurable Service Class Access Bandwidth—The allocation of the access interface aggregate bandwidth among service classes will be configurable through the service portal. Ingress traffic policing will enforce the allocation within each service class, and egress traffic policing (inelastic/real-time) or shaping (preferred elastic and elastic classes) will manage bandwidth within each service class based on information priority. Default service will be best effort (100 percent allocation to the elastic service class) for customers that do not require CoS-enabled service assurance.

Service Offering	Secret IP Data (also known as SIPRNet)
Service Lifecycle Status	Maintain & Sustain
Security Classification	Up to and including Secret
Service Performance	Service performance is measured, monitored, and reported as defined in the DISN Telecommunications Service Level Agreement, which can be found on the DISA Direct Home page at <u>https://www.disadirect.disa.mil</u>
Service Rates	Service rate information can be found on the DISA Direct Home page at <u>https://www.disadirect.disa.mil</u> under Inventory and Billing.
Connection Approval	There are services that require a connection approval. Information regarding connection approvals can be found at the <u>DISN Connection Process</u> Web site.
Rate this Page Click here to rate this page	

Using the SIPRNET

The Secret Internet Protocol Router Network (SIPRNET) is the Department of Defense's largest network for the exchange of classified information and messages at the SECRET level. It supports the Global Command and Control System, the Defense Message System, and numerous other classified warfighting and planning applications. Although the SIPRNET uses the same communications procedures as the Internet, it has dedicated and encrypted lines that are separate from all other communications systems. It is the classified counterpart of the Unclassified but Sensitive Internet Protocol Router Network (NIPRNET), which provides seamless interoperability for unclassified combat support applications and controlled access to the Internet.

Access to the SIPRNET requires a SECRET level clearance or higher and a need to have information that is available only on the SIPRNET. Because the SIPRNET is an obvious target for hostile penetration, a number of strict security procedures are applied. All users must be approved and registered. Passwords must be changed at least every 150 days and must have at least 10 characters including two upper case letters, two lower case letters, two numbers, and two special characters. When a person is using the SIPRNET, he/she must not leave the workstation unattended.

A computer with a non-removable hard drive used to access the SIPRNET must be located in an area approved for open storage of SECRET information. A computer with a removable hard drive does not have to be in an open storage location, but the hard drive must be appropriately marked with the classification of the material it contains and, when not in use, must be removed and stored in a container approved for the storage of SECRET information. If physical keys are used, they will be numbered and stored in a container approved for the storage of SECRET material.

Linking a computer with access to the SIPRNET to the Internet or to any other computer or media storage device that has not been approved for use with SECRET information is a serious security violation. Once any media storage device such as a CD, floppy disk, or memory stick has been connected to a computer with access to the SIPRNET, it becomes classified at the SECRET level. It must be protected accordingly and shall not be used on any unclassified computer. Classified information retrieved from the SIPRNET should not be accessed via NIPRNET

Technological advances in storage devices are making it easier for

classified information to be removed from secure areas. Data-storage devices such as Personal Digital Assistants (PDA), Key-chain drives, Memory watches etc, should not be allowed in an environment where classified information is processed because of their infrared and similar recording capabilities. For computers used to process classified information, it is recommended that infrared (IR) port beaming capability be disabled. If the IR port is unable to be disabled, cover the IR port with metallic tape.

A SIPRNET workstation cannot be attached to a shared or networked NIPRNET printer. It can only be attached to a local printer directly connected to the workstation in a secure area. You are responsible for ensuring that all classified printed material is properly marked and for complying with appropriate procedures for removing that material from the vaulted or other secure area. Personnel with access to the SIPRNET must receive security awareness training at least once a year tailored to the SIPRNET system and the kinds of information accessed on that system.

The SIPRNET system maintains an audit trail of all users. This includes the identity of all persons accessing or attempting to access the SIPRNET, date and time of logon/logoff, and any noteworthy activities that might indicate an attempt to modify, bypass, or negate security safeguards.

HOME | CLASSIFIED INFORMATION CONTENTS | TOP OF PAGE | HELP INFORMATION | CONDUCT | THREATS | TECH VULNERABILITY | ASSISTANCE SPY STORIES | TREASON 101



SECRET Internet Protocol Router Network (SIPRNET)

22 June 2004

Kimberly K. Reed ISEC FDED

Explanation of SIPRNET

• The SIPRNET is the Defense Department's communications backbone, used for passing tactical and operational information at the secret classification level. The Joint Staff J-6 and the National Security Agency, Defense Intelligence Agency and Defense Information Systems Agency directors administer the SIPRNET jointly. These officers are called the SIPRNET designated approving authorities. They and their representatives (normally the Defense Information Systems Network Security Accreditation Working Group) manage the shared risk of the SIPRNET system and decide who can connect when, where and how.

Requirement for SIPRNET

- Depending upon your unique situation, SIPRNET may be installed in several ways:
 - Site must have SIPRNET POP (must arrange for this circuit through DISA)
 - KIV / TACLANE / Sectera end equipment (used to extend the SIPRNET circuit to user)
 - Protected Wire Distribution may be required (when the user is not in the same room as the encryption equipment)

Example of SIPRNET (at POP)

KG-175 E100/Classic SIPRNET Bldg 2101 SM FIBER B TCC ROOM G-5A MM_FIBER Α -----Demarcation Media SM FIBER SM FIBER Converter TACLANE *Carrier CISCO KIV-7/ KIV-19 DSU E100 To Bldg 2101 Equipment* To Bldg 600 7206 ROUTER м T-1 From DISA SERIAL Army DISA PROVIDED W/ (DOIM PROVIDED) Fiber RED & BLACK CABLE Connect using Fast USERS Ethernet port TCC SIPRNET POP

A DENOTES BUILDINGS

West Point Proposed SIPRNET Extension using TACLANE/

NOTE: SMALL LOCKING CABINET IN EACH USER OFFICE

Example of SIPRNET (at User)

West Point Proposed SIPRNET Extension using TACLANE/ KG-175 E100/Classic



NOTE SMALL LOCKING CABINET IN EACH USER OFFICE

SIPRNET References

- Army Regulation 25-1, Army Information Management, 31 May 2002 (http://www.army.mil/usapa/epubs/pdf/r25_1.pdf)
- Army Regulation 25-2, Information Assurance, 14 November 2003 (http://www.army.mil/usapa/epubs/pdf/r25_2.pdf)
- Army Regulation 380-5, Department of the Army Information Security Program, 29 September 2000 (http://www.army.mil/usapa/epubs/pdf/r380_5.pdf)
- Army Regulation 380-19, Information Systems Security, 27 February 1998 (http://www.fas.org/irp/doddir/army/r380_19.pdf)
- NSTISSAM TEMPEST/2-95, Red/Black Installation Guidance, 12 December 1995 (http://cryptome.sabotage.org/tempest-2-95.htm)
- NSTISSI No. 7003, Protective Distribution Systems (PDS), 13 December 1996 (http://www.nstissc.gov/Assets/pdf/nstissi_7003.pdf)
- SIPRNET Customer Connection Process Guide, 19 June 2003

FDED Capabilities

- The Fort Detrick Engineering Directorate provides engineering and installation assistance at the request of Army DOIMs and other customers who require SIPRNET extensions.
 - Engineering design with cost estimate for implementation of secure data communication links .
 - Implementation / installation of the SIPRNET extension.
 - If you would like to "hire" ISEC for your SIPRNET needs, please contact Mike Dayhoff (DSN 343-6406) or Cal Farrar (DSN 343-6417).