Non-Secure Internet Protocol Router Network (NIPRNET)

(Current DISA term: Sensitive but Unclassified (SBU) IP Data)

Proficiency Code: A

The SBU IP Data service also provides DoD customers with centralized and protected access to the public internet. NIPRNet provides support to SBU IP Data telecommunication services for combat support applications to the DoD, Joint Chiefs of Staff (JCS), Military Departments (MILDEPS), Combatant Commands (COCOM), and senior leadership. It provides seamless, interoperable, common user IP services to customers with access data rates ranging from 56 kilobits per second (Kbps) to 2.4 gigabits per second (Gbps) via direct connections to a NIPRNet router, and services to the Tactical community via Integrated Tactical-Strategic Data Network / Standard Tactical Entry Point (ITSDN/STEP) sites. It also provides access to the internet through controlled Internet Access Points.

(The NIPRNet Hardening program is a Defense-in-Depth Information Assurance (IA) and Computer Network Defense (CND) effort designed by DISA to satisfy some, but not all, of the requirements specified by CJCSM 6510.0. The NIPRNet Hardening Program consists of several projects that together will improve the defensive posture of all unclassified DoD networks. The Web Content Filter (WCF) program is one of the associated NIPRNet hardening programs. WCF provides boundary protection at the application layer for web (HTTP/HTTPS) traffic and provides URL filtering for requests and malware filtering on responses. WCF program efforts will assure mission execution in the face of cyber-attack by reducing the NIPRNet attack surface and improving information to attack diagnosis, detection, and response (A2DR) systems. The WCF will provide uniform protections for clients against web vulnerabilities. This unclassified IP data service for internet connectivity and information transfer supports DoD applications such as email, web services, and file transfer. The SBU IP Data service also provides DoD mission partners with centralized and protected access to the public internet. This service supports up to and including SBU security classification.

In addition, the NIPRNet Federated Gateway (NFG) architecture implements enterprise capabilities that support additional DoD-wide solutions that protect against dangerous protocols, secure DoD-wide Domain Name Service (DNS), and secure enterprise-wide support to the teleworking workforce. This creates a clear boundary between DoD and others; enables improved sharing with key partners; and focuses cyber-attack detection, diagnosis, and reaction on the most important DoD missions. This gives DoD some ability to maneuver at the boundary in response to cyber-attacks.

Source Material: https://storefront.disa.mil/kinetic/disa/service-catalog#/forms/sensitive-but-unclassified-internet-protocol-data