Enterprise Systems

Proficiency Code: A

Looking at the enterprise networks employed throughout the Air Force and DOD, we will begin our discussion at the top level of all DOD communications. This is the DODIN.

Department of Defense Information Network

The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The DODIN includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve information superiority. The DODIN supports the Department of Defense, National Security, and related Intelligence community missions and functions (strategic, operational, tactical, and business), in war and in peace. The DODIN provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The DODIN provides interfaces to coalition, allied, and non-DOD users and systems.

Services

DODIN consists of several components that provide key services. They are access, transport, application, voice, video, satellite communications, and aerial layer services. Let us begin with the access services.

Access services

Access services of the DODIN divides into two elements; the DISN Interface and the DOD Gateway.

Defense Information Systems Network Interface

The DISN is the major element of the DODIN (fig. 3–3). The DISN has three segments: sustaining base, long haul, and deployed. The DISN is DOD's worldwide enterprise-level telecommunications infrastructure providing end-to-end information transfer for supporting military operations. For the most part, it is transparent to the joint force. The DISN facilitates the management of information resources and is responsive to national security, as well as DOD needs. It provides basic DODIN services to DOD installations and deployed forces. Those services include voice, data, and video, as well as ancillary *enterprise services* such as directories and messaging. DOD policy mandates the use of the DISN for wide area and metropolitan networks.

Department of Defense Gateway

In concert with military and commercial communication segments that support DOD missions, the primary interface point between the sustaining base and deployed forces is the DOD

Gateway. The DOD Gateway may include the standardized tactical entry point and upgrades called the Teleport and the Modernization of Enterprise Terminal programs. The DOD Gateway provides robust worldwide ground entry interface to SATCOM resources and DISN services. The design of the DOD Gateway meets the requirement of the provisioning of pre-positioned, sustainable DISN services. An equally important result of this upgrade to the DISN has been the improvement and standardization (facilitating interoperability) of the JFC's access to the DISN.

The DOD Gateway program enhances the ability of the DISN to respond to the needs of the joint force. Joint and service-level operational users rely on both military and commercial SATCOM systems to support their communications requirements. The DOD Gateway provides predefined support packages on a predefined timeline. This support extends via common user transports and includes voice, data, and video services. These services extend directly to deployed naval forces and to each component of a JTF, if employed. Voice services include access to the DSN and the Defense Red Switched Network. Data will include access to the SIPRNET and the NIPRNET. Video services include access to DISN video services. It will also support the JWICS, a Secret Compartmentalized Information (SCI)-level data, voice, and video services network.

Although implemented globally, the DOD Gateway is under a single executive agent. JFCs and their staffs play an important role in DOD Gateway employment. The tactical communications system planners coordinate entry point access and procedures. DISA plays a major role in the planning process and utilizes regional contingency exercise planning branches, the United States Cyber Command (USCYBERCOM)-operated Joint Operations Center and DISA's DODIN operations center to facilitate that interaction with the joint force. DOD Gateway (fig. 3–4) has evolved to incorporate satellite connectivity through the Teleport program. This provides greater flexibility in the use of DOD and commercial SATCOM resources. Flexibility does not imply additional bandwidth for the deployed joint force. However, use of quad-band terminals provides the joint force with more flexible means of SATCOM support.

The DOD Teleport Program is an upgrade of satellite telecommunication capabilities at selected DOD gateways to improve DISN service access to the deployed joint force.

Voice services

DODIN voice services include the following that will be discussed later in further detail.

• Defense Switched Network.

• Defense Red Switched Network.

• Enhanced Mobile Satellite Services.

• Tactical Voice.

• Voice over Internet Protocol and Voice over Secure Internet Protocol services.

Transport services

• NIPRNET.

• SIPRNET.

• JWICS.

• Multi-national WAN, which is an information network supporting the multi-national operations that may be unclassified or classified.

The Joint Data Network (JDN) carries tactical data link (TDL) and multi-sensor early warning information in support of joint operations. Information passes over the JDN in near real time. The JDN consists of the multi-TDL network, ground network, intelligence network, and sensor network along with other feeds. Effective design and implementation of the multi-TDL network are critical in managing complexities to improve the JFC's ability to engage hostile forces and prevent friendly fire.

Applications

The Global Command and Control System-Joint (GCCS-J), the Theater Battle Management Core Systems (TBMCS), the Army Battle Command System, DOD enterprise collaboration service, and the Automated Message Handling System (AMHS) discussed are illustrative of applications incorporated into the DODIN.

Video services

Video services include the defense VTC system, the Secret Compartmentalized Information VTC system, and commercial news feed capability.

Defense video teleconferencing system—Global

The defense VTC system–global is a classified, closed video network capable of voice, image, and data exchange supporting command and control (C2) functions of DOD. It utilizes industry standard technology for robust interoperability to commercial systems as well as legacy DOD systems.

Secret Compartmentalized Information-level video teleconferencing

The SCI-level VTC system is a classified, closed video network capable of voice, image, and data exchange supporting intelligence and C2 functions of DOD.

NOTE: The JWICS network typically carries the SCI VTC data.

Commercial news feed

Commercial news feeds may be rebroadcast over DOD communications systems or received via a commercially leased terminal in support of C2 functions.

Satellite communication

SATCOM is a critical segment of the DODIN that provides the ability to establish or augment the communications system in regions of the world that lack suitable terrestrial infrastructure, such as polar regions, open ocean, and remote areas of the world.

Aerial layer

The aerial layer provides additional communications capacity by using manned and unmanned systems to host communications packages for continuous communications coverage of large geographic areas. The aerial layer integrates with the space a terrestrial network segments to enable advanced information exchange capabilities.

Defense Information System Network

The DISN is a telecommunications network that provides the exchange of information in an interoperable and global space, divided by security demands, transmission requirements and geographic needs of targeted end-user customers. The DISN offers a selection of integrated standards-based services to fulfill these connectivity needs.

These services provide a framework of protocols used by the DOD to support diverse telecommunication requirements for its organizations. DISN is functionally broken down into seven sub-groups. The sub-groups are content delivery, data, messaging, satellite, transport, voice, and VPN. These sub-groups further divide into functional areas.

Content delivery

If you use the DODIN for anything, you have leveraged the Global Content Delivery Service (GCDS) without even realizing it.

Global Content Delivery Service

GCDS leverages commercial Internet technology to accelerate and secure DOD Web content and applications across the NIPRNet, SIPRNet, and other DOD ISs. GCDS's global platform of hundreds of specially equipped servers helps the DODIN withstand the crush of daily requests for rich, dynamic, and interactive content, transactions, and applications. When delivering on these requests, GCDS detects and avoids DODIN related problem spots and vulnerabilities to ensure mission critical software downloads flawlessly and applications perform reliably. The same platform also secures critical applications using its Web application firewall, allowing it to inspect Web requests and detect application attacks before an organization's Web server and data center is exposed to a possible threat. Furthermore, GCDS provides customers and security response teams with vital information that can be used to detect and block anomalous and potentially malicious attacks. Overall, GCDS provides the best user experience possible by not only increasing performance and availability anytime, anywhere for the warfighter, but also enhancing the security posture of an organization's data center to ensure customer's data is secured 24x7.

GCDS offers these features to the DOD:

• Improved delivery of mission content to warfighters globally.

• Capacity on-demand to meet peak loads – without added IT infrastructure.

• Increase user adoption by improving user experience and minimizing response times.

• Reduced infrastructure costs, while meeting mission requirements.

• Top notch 24x7 service and support from commercial and government experts.

Data

Three data services within DISN are Sensitive but Unclassified IP Data (SBU IP), Secret IP Data, and Top Secret/Sensitive Compartmented Information Data (TS/SCI IP Data). Be aware that this list is not all encompassing and as technologies emerge, it will expand.

Secure but Unclassified Internet Protocol data

SBU IP data or NIPRNet provides point-to-point connectivity to the DOD. This unclassified IP data service for Internet connectivity and information transfer supports DOD applications such as e-mail, Web services, and file transfer. The service also provides DOD customers with centralized and protected access to the public Internet.

Secret Internet Protocol data

Secret IP data service or SIPRNet provides point-to point connectivity to the DOD. It also provides IP-based secret information transfer across DOD networks for official applications such as e-mail, web services, and file transfer. The Secret IP Data service gateway 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 intranets and centralized gateway external network information exchange (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.

NOTE: The customer must provide encryption devices for connection to the Secret IP Data service.

Top Secret/Secret Compartmentalized Information IP Data

Top Secret/Secret Compartmentalized (TS/SCI) IP Data or JWICS service is a secure high-speed multimedia communication service between SCI users designed to support the Department of Defense Intelligence Information System (DODIIS) community through the Defense Intelligence Agency (DIA) Regional Support Centers (RSC). As its name implies, TS/SCI IP Data supports classification up to and including top secret.

Messaging

Currently DISA only offers one messaging service, the Organizational Messaging Service (DMS).

Organizational Messaging Service

The DMS provides a range of assured services to the customer community that includes the military services, DOD agencies, combatant commanders (COCOM), non-DOD US government

activities and the IC. These services include the ability to exchange official information between military organizations and to support interoperability with allied nations, non-DOD activities and the IC operating in both the strategic/fixed-base and the tactical/deployed environments.

Satellite

The satellite services that serve the DOD include commercial satellite service and international maritime satellite.

Commercial satellite service

Commercial satellite service (CSS) uses a number of different satellite services to provide warfighters with worldwide access and Global Information Grid (GIG) connectivity for diversity, redundancy, and availability. DISA is the DOD's only authorized service provider for commercial fixed satellite services and mobile satellite services. DISA also serves as an advocate for the use of commercial Satellite communication in order to increase the availability and flexibility of military communications.

CSS allows for the lease or acquisition of terminals, teleports, landlines, operations and maintenance (O&M) support, host-nation support and approvals (e.g., negotiation support services, host-nation approvals, landing rights, frequency clearance, terminal registration, licenses, authorization to operate the terminals), engineering and any other communications resource that a customer requires providing for a true end-to-end, turnkey solution.

Warfighters gain access to SBU IP Data, Secret IP Network Data, TS/SCI IP Data, SBU Voice and Multilevel Secure Voice to meet their voice and data requirements.

International Maritime Satellite

International Maritime Satellite (INMARSAT) is a pre-existing, pre-engineered Mobile Satellite Services (MSS) billed on a per usage basis. It uses IP-based Broadband Global Area Network (BGAN), Fleet Broadband (maritime), and Swift Broadband (aeronautical) services, as well as a range of legacy services. Services are available through blanket purchase agreements (BPA).

These services include commercial satellite airtime and equipment for voice and data communications; land-mobile or ship-to-ship, ship-to-shore, shore-to-ship, and air/ground/air services on a global basis, including calls made to foreign earth stations and transparent connectivity into the existing PSTN.

Transport

Dedicated transport service is a private-line transport service that provides point-to-point connectivity to mission partner locations. DISN offers several key features for long haul communication. Dedicated transport service offers the ability to carry multiple classifications of traffic over the same circuit, low and constant latency. In addition, it offers efficient use of bandwidth and wide geographic deployment, which reduces leased-line distance and cost. Lastly, it offers up to and including TS/SCI classification.

Voice

Two of the more common DISN voice services are SBU Voice, and VoSIP.

Sensitive but Unclassified Voice

SBU Voice provides IP (Voice over IP) and circuit-switched (Public Switched Telephone Network) voice-band data transfer and dial-up videoconferencing.

SBU Voice services also provide automated access capabilities to the following networks:

• International gateways to the defense networks of our allies for cost avoidance of international commercial calling.

• Enhanced Mobile Satellite Services (EMSS).

• Government Emergency Telephone System (GETS).

Voice over Secure Internal Protocol

The VoSIP service provides a cost-effective, reliable and secure means of classified voice communications, secret only, for C2 and non-C2 customers with the capability to communicate directly using point-to-point or conference calling. It does provide a media/voice interface (gateway) to the circuit-switched network providing interoperability between the VoSIP service and the Multilevel Secure Voice service.

VoSIP provides:

• An interface between the IP telephony and the circuit-switched network.

• A full range of supplemental user features available for IP telephony (e.g., call hold, call transfer, and abbreviated dialing.)

• A separate IP address space for voice communications

• Firewalls at each VoSIP site and access control lists on all routers to ensure that only permitted traffic flows.

• Secure voice communication up to and including Secret.

Virtual private networks

A VPN extends a private network across a public network, like the Internet. A VPN establishes a virtual point-to-point connection using dedicated connections, virtual tunneling protocols or traffic encryptions. DISA provides a multitude of VPN services over the DISN; see the VPN protocols in use listed below.

• Private IP Service.

• Private LAN Service.

• Label Transport Service.

• Medical Community of Interest (MEDCOI).

• Common Mission Network Transport (CMNT).

• DISN Test and Evaluation Service.

• Joint Information Environment-Joint Regional Security Stack (JIE-JRSS) Community of Interest VPN.

Networks and infrastructure

This lesson will present you with different types of networks and their infrastructure. Those networks are the Base information Transport Infrastructure (BITI), NIPRNET, SIPRNET, JWICS, National Security Agency Net (NSANet), Defense Switched Network (DSN), and Defense Red Switch Network (DRSN).

Base Information Transport Infrastructure

BITI is a part of the Air Force Information Network (AFIN). The BITI program divides into two different systems: BITI-Wired and BITI-Wireless. These programs provide the networking infrastructure, management mechanisms, security features, and associated services for voice, data, video, sensor, control, and other forms of wired and wireless electronic communications on the AFIN. The BITI-Wired Program procures, installs and sustains Base Infrastructure (BI) requirements (e.g., routers, switches and transmission links). The BITI-Wireless Program is responsible for providing wireless communications capabilities to the local base.

Non-secure Internet Protocol Router Network

DISA recently renamed NIPRNET to SBU IP Data. It still provides the same basic services of point-to-point connectivity to DISA mission partners. This unclassified IP data service for Internet connectivity and information transfer supports DOD applications such as e-mail, Web services, and file transfer. 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, JCS, military departments (MILDEPS), COCOM, and senior leadership. It provides seamless, interoperable, common user IP services to customers with access data rates ranging from 56 Kbps to 2.4 GB/s 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.

Secret Internet Protocol Router Network

Just like NIPRNet, SIPRNET is now referred to as Secret IP Data. This service also provides point-to-point connectivity to mission partners. SIPRNet/Secret IP Data provides IP-based secret information transfer 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, IC and allied information at the secret level.

The Secret IP Data service includes IP-based secret information exchange within DOD (intranet) and centralized gateway external network information exchange (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.

SIPRNet is DOD's largest interoperable C2 data network supporting the Global Command and Control System (GCCS), the DMS, collaborative planning and numerous other classified warfighter applications. SIPRNet provides secure, seamless, interoperable, and common user packet-switched data communications services to mission partners with access data rates ranging from 56 Kbps to 1.0 Gbps. Remote dial-up services are available up to 115 Kbps and services to the tactical community are available via ITSDN/STEP sites.

Joint World-wide Intelligence Communications System

JWICS provides a transmission path capable of secure video/data within the defense intelligence community. JWICS is the sensitive compartmented information portion of the DISN. It incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing.

JWICS provides transmission of imagery files and intelligence documents rapidly between sites; real time two-way video teleconferencing; receipt of the intelligence community's TV broadcast of the Defense Intelligence Network (DIN); and connectivity to the Joint Intelligence Virtual Architecture (JIVA). It provides 24-hour TS-SCI multimedia communications to include secure VTC.

National Security Agency Net

NSANet is the NSA's internal classified network. The network is a highly secured computer network consisting of fiber-optic and satellite communication channels almost completely separated from the public Internet. The network allows NSA personnel and civilian and military intelligence analysts anywhere in the world to have access to the agency's systems and databases. This access is tightly controlled and monitored.

Defense Switched Network

The DSN is a rapid, reliable, survivable, telecommunications network serving DOD authorized users. The DSN is a sub network of the DISN and DODIN. The basic DSN is a worldwide hierarchal network of telecommunication switches to which end instruments are connected. It provides rapid, reliable, survivable, non-secure, secure, and economical C2 telecommunications to selected users. To take advantage of economies of scale, the DSN also provides service to non-C2 users as long as the primary mission supporting C2 users is not impacted.

The DSN is only for official business or in the interest of the US Government and the first choice for all switched voice and dial-up video telecommunications between DOD user locations. The primary function of the DSN is to provide non-secure dial-up voice service. The DSN provides, via Secure Telephone Unit (STU), STE, and other Secure Communications Interoperability Protocol (SCIP) terminal equipment an additional source of secure communications for DRSN

users. A direct interface between DSN to DRSN allows extended DRSN communications to C2 users connected to DSN end offices (EO).

Defense Red Switch Network

The DRSN provides high-quality, secure telecommunications for C2 and crisis management. The DRSN uses cryptographically secured backbone trunks and access interfaces to provide user-dialed secure connections among senior DOD, civil, and allied decision makers within the following user communities:

• The President/Secretary of Defense/Chairman of the Joint Chiefs of Staff.

• National Military Command Center (NMCC).

• Airborne Command Post community.

• Combatant commands.

• Military Departments and subordinate organizations (military and civilian).

• Some US Government departments and agencies (e.g., Department of State).

• Some allies of the United States.

The DRSN is the primary network for secure conferencing and is the host network for the World Wide Secure Voice Conferencing System (WWSVCS) conferees, DSCS based Enhanced Pentagon Capability (EPC) conferences, and the Military Strategic and Tactical Relay Satellite (MILSTAR) based Survivable Emergency Conferencing Network (SECN).