

Term	Acronym	Definition
Access Control List	ACL	A table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file. Each object has a security attribute that identifies its ACL.
Air Blown Fiber	ABF	A scalable, easily configured fiber optic infrastructure that allows fiber to be blown through cabling pipes from one location to another. This system enables installers to update fiber in a matter of moments instead of hours or days.
Billing Account Code	BAC	A code assigned to customers to facilitate the billing process for telephonic services.
Blanket Purchase Agreement	BPA	Contracting vehicles that enable agencies to obtain services using a single pricing structure, thereby simplifying the billing process and reducing the number of contracts.
Bridge		A bridge connects equipment at various locations, with various speeds and with various protocols – via a digital network. ITA’s video teleconferencing bridges provide a conduit to Defense Video Services-Global (DVS-G) for customer sites that do not have a requisite site ID.
Cold Transfer		A phone call that comes in without any warning or explanation from the person who transferred the call. In the context of a service call, this means that a customer is transferred to a higher service tier without any interaction or transfer of information between the current tier and the next highest tier.
Commercial Off-the-Shelf	COTS	Software or hardware products that are ready-made and available for sale to the general public. COTS products are designed to be easily implemented into existing systems without the need for customization.

Common Information Technology	CIT	A range of services typically provided by an IT service supplier to multiple organizations and customers. CIT includes Operation and Maintenance, technical upgrade, engineering, integration, architecture, and information assurance of the infrastructure needed to provide the services.
Computer Network Defense Service Provider	CNDSP	Computer Network Defense is used to describe the actions taken (within the DoD) to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks. The CND service providers are those entities providing these services.
Connection Approval Package	CAP	Package required to obtain access to the Pentagon Unclassified or Classified backbone network (upon approval). Once granted access, the customer must provide ITA with any significant changes that affect the accuracy of the customer's CAP.
Continuity of Operations	COOP	An organization's ability to survive and sustain critical core business operations and functions during an unforeseen Enterprise interruption event.
Core Service		Standalone services offered by ITA to its customers. Core Services are enhanced by additional services that complement the Core Service. (These services are intrinsic to the Core Service and are provided to all subscribing customers.) Additionally, ITA may offer Elective Services to complement each Core Service.
Customer Account Manager	CAM	An organization's primary point of contact with its customers. CAMs resolve service-related issues and sign-up customers for new services.
Defense Satellite Communications System	DSCS	The workhorse of the U.S. Military's super-high frequency communications. DSCS provides military communications to troops in the field as well as commanders at multiple locations. DSCS III, the most recent configuration, provides uninterrupted secure voice and

Defense Information Systems Agency	DISA	A DoD combat support agency under the direction of the Assistant Secretary of Defense for Networks and Information Integration [ASD (NII)]. DISA is responsible for planning, engineering, acquiring, fielding and supporting global net-centric solutions and operating the Defense Information System Network (DISN) to serve the needs of the President, Vice President, Secretary of Defense, Joint Chiefs of Staff, Combatant Commanders and other DoD components under all conditions of peace and war.
Defense Information Systems Network	DISN	DoD's worldwide, common-user telecommunications network. DISN interfaces with customer-owned equipment to deliver secure and non-secure information from desktop to foxhole. DISN supports the Defense Message System (DMS) and Electronic Commerce/Electronic Data Interchange (EC/EDI).
Defense Red Switch Network	DRSN	A global, secure voice service that provides the President, Secretary of Defense, Joint Chiefs of Staff, combatant commanders and selected agencies with command and control secure voice and voice-conferencing capabilities up to the Top Secret SCI level.
Defense Switch Network	DSN	A worldwide private-line telephone network. Multilevel precedence and preemption capabilities on the DSN utilized by Command and Control (C2) users ensure that the highest-priority calls achieve connection quickly, especially during a crisis situation. The DSN also provides global data and video services using dial-up switched 56 kbps or 64 kbps Integrated Services Digital Network (ISDN) services.
Delegated Approval Authority	DAA	The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.
Demilitarized Zone	DMZ	A firewall configuration for securing local area networks (LANs).

Department of Defense Information Assurance Certification and Accreditation Process	DIACAP	A streamlined and modern certification and accreditation (C&A) process that complies with FISMA, is more compatible with DOD's IA controls-based approach for information systems security, and lends itself to the use of evolving automated C&A tools.
Elective Service		Optional services that enhance a given Core Service by adding features and/or increasing the capability of an existing service element.
Emergency Alert Services	EAS	A system used by government to send alerts via broadcast stations and cable systems.
Enterprise Management System	EMS	A Management System Platform that receives inputs from various, independent network and element management systems, and serves as a single monitoring point.
Federal Telecommunications Systems contract	FTS2001	A contractual vehicle that enables agencies to get worldwide telecommunications solutions, including voice, data, wireless, and video. Flexibility is built into FTS2001 to provide access to new technologies as they become available.
Fibre Channel		A technology for transmitting data between computer devices at data rates of up to 4 Gbps . A fibre channel is especially suited for connecting computer servers to shared storage devices and for interconnecting storage controllers and drives.
Fibre Channel Transport	FCT	A high-speed transport technology used to build storage area networks (SANs). Although fibre channel can be used as a general-purpose network carrying ATM, IP and other protocols, it has primarily been used for transporting SCSI traffic from servers to disk arrays.
Fortezza Certificate		Fortezza is a set of security algorithms used by the U.S. government.

Global Information Grid	GIG	A net-centric system operating in a global context to provide processing, storage, management, and transport of information to support all DoD, national security, and related Intelligence Community missions and functions (strategic, operational, tactical, and business) in war, in crisis, and in peace.
Gray Phone		A closed, SCI cleared, telephone network serving the Intelligence Community. The formal name for Gray Phone is the National Secure Telephone System (NSTS).
Information Assurance Vulnerabilities	IAV	Computer application software or operating system vulnerabilities, determined by NetDefense or DoD-Cert, a division of the Global Network Operations Center, of the JTF-GNO. These selected vulnerabilities are the mandated baseline, or minimum configuration of all hosts residing on the GIG framework.
Information Assurance Vulnerability Alert	IAVA	The comprehensive distribution process for notifying the Components about vulnerability alerts and countermeasures information.
Information Technology Infrastructure Library	ITIL	A globally recognized collection of best practices for IT service management.
International Organization of Standards	ISO 9001-2000	Specifies requirements for a Quality Management System overseeing the production of a product or service. It is not a standard for ensuring a product or service is of quality; rather, it attests to the process of production, and how it will be managed and reviewed.
Intrusion Detection System	IDS	IDSs inspect all inbound and outbound network activity and identify suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.
Intrusion Prevention System	IPS	An IPS keeps systems safe by identifying and blocking suspicious traffic.

Joint Task Force-Global Network Operations	JTF-GNO	Directs the operation and defense of the Global Information Grid (GIG) across strategic, operational, and tactical boundaries in support of the U.S. DoD's full spectrum of war fighting, intelligence, and business operations.
Joint Worldwide Intelligence Communications System	JWICS	A network designed to meet the requirements for secure (TS/SCI) multi-media intelligence communications worldwide. JWICS replaces the DDN DSNET3 as the Sensitive Compartmented Information (SCI) component of the Defense Information System Network (DISN).
Lean Six Sigma		Lean Six Sigma combines the industry best practice principles of Lean manufacturing and Six Sigma. Six Sigma is a system of practices originally developed to systematically improve processes by eliminating defects. Lean is a generic process management philosophy renowned for its focus on reduction of waste in order to improve overall customer value.
Local Area Network	LAN	A group of computers and associated devices that share a common communications line or wireless link. Typically, connected devices share the resources of a single processor or server within a small geographic area.
Malware Behavioral Analysis		Malware Behavioral Analysis examines how the malicious programs interact with their environment: the file system, the registry (for Windows programs only), and the network.
Mean Opinion Score	MOS	In voice communications, particularly Internet telephony, the mean opinion score provides a numerical measure of the quality of human speech at the destination end of the circuit.
Metropolitan Area Network	MAN	A network that interconnects users with computer resources in a geographic area or region larger than that covered by a large local area network (LAN), but smaller than the area covered by a wide area network (WAN).

Move, Add, or Change	MAC	The capability to move, add, or change a specific aspect of a service. (e.g. Moving a network port from one office to another)
National Capital Region	NCR	The District of Columbia; Montgomery, Prince George's, and Frederick Counties in Maryland; Arlington, Fairfax, Loudon, and Prince William Counties in Virginia; and all cities within the outer boundaries of the combined area of the aforementioned counties. The NCR is defined in Executive Order 13150 (21 Apr 2000).
National Communications System	NCS	The mission of the NCS is to assist the President, the National Security Council, the Homeland Security Council, the Office of Science and Technology Policy and the Office of Management and Budget in the coordination of planning for, and provisioning of, national security and emergency preparedness communications for the Federal Government (under all circumstances, including crisis or emergency, attack, recovery and reconstitution).
Network Enterprise Center	NEC	The NEC ensures that enterprise services (e.g. e-mail, user storage, office automation, collaboration, information assurance, etc.) are implemented and managed in accordance with current policy, procedural guidance, and management procedures.
Network Access Point	NAP	A major point of access to the internet.
Network Systems Management Center	NSMC	A 24 x 7 service desk providing support to customers receiving Cable Television service.

Non-Global Information Gig Services	Non-GIG Services	Circuit Transport Services provided by ITA (or locally procured by an organization) that are not considered part of DISA's GIG. Non-GIG services provided by ITA ride over ITA's managed backbone and other associated transport equipment.
Operations and Maintenance	O&M	The range of activities and services provided for the upkeep and preservation of the existing systems and facilities.
Operations Support		Operations-oriented service elements that are provided in support of (or as an enhancement to) each ITA customer's IT service.
Penetration Testing		Security-oriented probing of a computer system or network to seek out vulnerabilities that an attacker could exploit.
Pentagon Area		Includes the Pentagon and Swing Space.
Pentagon Computer Incident Response Team	PENTCIRT	Assists with minimizing the consequences of computer incidents, including malicious logic, and facilitates the return of compromised network resources to acceptable levels of confidentiality, integrity, and availability.
Pentagon Renovation	PENREN	A multi-year, multi-phased program to renovate the Pentagon building.

Pentagon Technical Control Facilities	PTCF	Provides the U.S. Army with operation and maintenance services for Pentagon telecommunications circuits.
Protected Distribution System	PDS	A wireline or fiber-optics telecommunication system that includes terminals and adequate acoustical, electrical, electromagnetic, and physical safeguards to permit its use for the unencrypted transmission of classified information.
Redundant Array of Independent Disks	RAID	A method for storing the same data in different places (thus, redundantly) on multiple hard disks. By placing data on multiple disks, input/output (I/O) operations can overlap in a balanced way, improving performance.
Remedy		An incident management ticketing system used to track reported issues from inception to resolution.
Remote Access Service	RAS	Provides state-of-the-art remote access connectivity to Pentagon network resources via dial-up or broadband connections.

Resource Situational Awareness Center	RSAC	Pentagon facility that provides for the collaboration of effort between the four services in supporting the joint staff and the service's Title 10 function. RSAC integrates the operations and intelligence divisions of the four services within a single area to coordinate efforts and share information in the event of a crisis (to include tsunamis, hurricanes, and attacks against the United States and its allies).
Resumption Point Objective	RPO	The maximum acceptable level of data loss following an unplanned "event", like a disaster (natural or man-made), act of crime or terrorism, or any other business or technical disruption that could cause such data loss. The RPO represents the point in time, prior to such an event or incident, to which lost data can be recovered (given the most recent backup copy of the data).
Resumption Time Objective	RTO	A period of time within which business and/or technology capabilities must be restored following an unplanned event or disaster.
Reverse Engineering		The process of discovering the technological principles of a device, object, or system through analysis of its structure, function and operation. Reverse engineering often involves taking something (e.g. a mechanical device, an electronic component, a software program) apart and analyzing its workings in detail, usually to try to make a new device or program that does the same thing without copying anything from the original.
Sensitive but Unclassified	SBU	A designation given to information that is generally restricted from public disclosure, but which is not classified.
Service Offering		A functional area of IT services that is comprised of interrelated Core Services, Elective Services and Operations Support. ITA has divided its Core Services into 13 Service Offerings.
Service Restoral		The mean time to restore service following system failures that result in a service outage. The time to restore includes all time from the occurrence of the failure until the restoral of service.

Storage Area Network	SAN	A high-speed sub-network of shared storage devices. A storage device is a machine that contains nothing but a disk or disks for storing data
Strategic Command	STRATCOM	Headquartered at Offutt Air Force Base, Nebraska, STRATCOM is one of nine U.S. unified commands under the DoD.
Swing Space		Temporary space provided by the Renovation Program (PENREN) for those displaced by the renovation effort. Swing Space outside of the Pentagon includes: FOB2, Navy Annex, 1500 Wilson Blvd; 1777 N. Kent St. Rosslyn (Rosslyn Plaza North) and Presidential Towers in Crystal City
Technical Analysis Cost Estimate	TACE	An estimate outlining the costs associated with a project. TACEs typically exceed the parameters of a MAC.
Telecommunications Service Order	TSO	The authorization from a DISA Allocation and Engineering (A&E) activity to start, change, or discontinue circuits, trunks, links, or systems; to amend previously issued TSOs; and to effect administrative changes. It is a document in most cases, although a verbal TSO may be
Telecommunications Service Priority	TSP	A Federal Communications Commission (FCC) program used to identify and prioritize telecommunications services that support National Security Emergency Preparedness (NS/EP) missions.
Tivoli Storage Manager	TSM	A tool that automates data backup and restore functions, and centralizes storage management operations.
Type 1 Encryption Device		A Type 1 encryption device is a device or system certified by the National Security Agency (NSA) for use in cryptographically securing classified U.S. Government information.
Uninterruptable Power Supply	UPS	A power supply that includes a battery to maintain power in the event of a power outage.
Virtual Machine (Ware)	VM	Used to partition x86-based workstations and servers into separate virtual machines, each containing its own copy of the OS. Supporting Windows, Linux and NetWare, VMware resides as a layer between the hardware and the virtual machine partitions.

Virtual Private Network	VPN	A network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.
War Dialing		A method of automatically scanning telephone numbers using a modem, usually dialing every telephone number in a local area to find where computers or fax machines are available, then attempting to access them by guessing passwords.
Warm Transfer		The practice of transferring escalated service calls by actively engaging the technician at the next highest tier prior to transferring the call. Typically, a warm transfer also includes the transfer of information gathered from the customer, so that the customer is not required to provide the same information twice.
Washington Interagency Telecommunications Services	WITS2001	The Washington Interagency Telecommunications Services contract through which ITA provides local telecommunications services for its customers.