CAPABILITY PRODUCTION DOCUMENT

FOR

UNITED STATES SPECIAL OPERATIONS COMMAND (USSOCOM)

TACTICAL LOCAL AREA NETWORK (TACLAN)

Increment:

ACAT: III

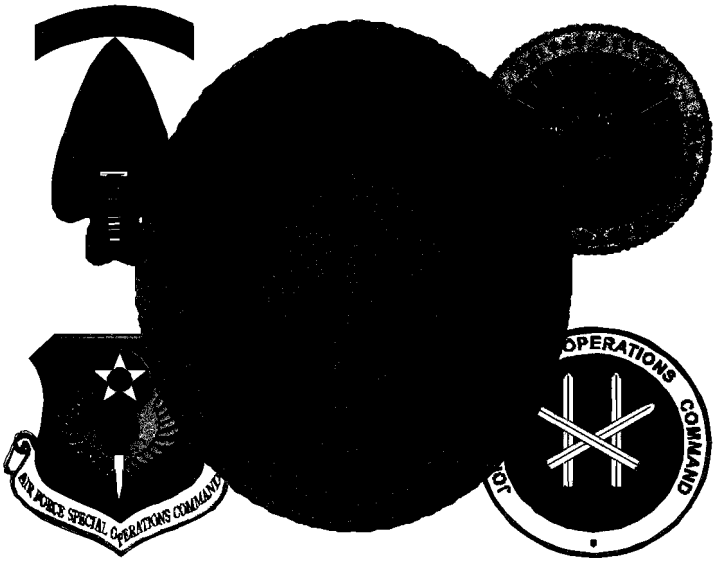
Validation Authority: Commander USSOCOM

Approval Authority: Commander USSOCOM

Milestone Decision Authority: USSOCOM Acquisition Executive

Designation: Independent

Prepared for:



22 March 2004

Executive Summary

The Tactical Local Area Network (TACLAN) program responds to limitations of deployed automation systems and networks and network interoperability and functionality limitations identified through user feedback and requirement statements. Implementing a managed approach to address operational shortfalls, TACLAN is needed to provide centralized program oversight to guide system-wide technology insertions and improvements, and preventing duplication of effort, limited commonality of systems, and piecemeal support arrangements for deployed forces.

TACLAN is the tactical equivalent of the SOF C4I Automation System (C4IAS) and a critical part of the SOF Information Enterprise (SIE). It will interconnect deployed SOF elements from the smallest team to a Joint Special Operations Task Force (JSOTF) headquarters with seamless, interoperable networks to share information, facilitate responsive knowledge based decisions, and provide an interface between the SOF Warfighter and the Global Information Grid (GIG). TACLAN is envisioned to be a modular, scalable suite of computer network equipment and workstations providing similar functionality to the garrison suites. The TACLAN evolutionary acquisition effort will integrate current and future USSOCOM tactical automated information systems into an efficient, deployable information management system supporting the interchange of knowledge among commanders, operators, and support personnel. TACLAN will support a wide range of functions including command and control, intelligence analysis and reporting, office automation, decision-making assistance, mission analysis, planning, rehearsal and execution support.

TACLAN is primarily a network infrastructure program, with some applications for common user functions. TACLAN infrastructure includes routers, hubs, switches, servers (file, mail, and proxy), network management and information assurance tools, printers, scanners, cabling, common user and special-purpose (i.e., mission planning, imagery, intelligence, etc.) workstations to interconnect deployed automation customers. TACLAN infrastructure also includes remote computing services to interconnect liaison elements and tactical teams to the main network, to include Field Computing Devices for tactical teams. On the applications side, TACLAN provides network connectivity, e-mail, information assurance, network management, and common user software applications in accordance with (IAW) the USSOCOM Common Information Technology Baseline List (CIBL). Common user software includes office applications (i.e., Word, PowerPoint, etc.), web services, collaboration tools, forms software, intelligence applications, and knowledge management services.

The TACLAN program will be the foundation for future USSOCOM tactical automation systems and services. It will use Commercial-off-the-Shelf (COTS) and Government-off-the-Shelf (GOTS) hardware and software to the fullest extent possible and will be compliant with industry and DOD standards while maintaining an open systems architecture. This will maximize interoperability and standardization and reduce costs associated with specialized military equipment. The TACLAN system will leverage Service tactical automation efforts wherever possible, and use MFP-11 funding to fill

gaps in Service provided programs. TACLAN associated systems migration objectives are tied to evolutionary acquisition practices that are Defense Information Infrastructure (DII)/Common Operating Environment (COE) compliant and include evolutionary technology insertions. Software development efforts will remain under other existing C4I programs. The USSOCOM CIBL will identify components for use in the TACLAN system. Required TACLAN hardware and software not presently on the CIBL will be submitted to the USSOCOM enterprise review board (ERB) for validation and approval. Intelligence requirements will be validated by the USSOCOM Intelligence System Requirements Management Council (ISRMC). As new requirements emerge for deployed SOF C4I, users will identify requirements, which will then be validated through a formal configuration control process.

Table of Contents

List of Tables

Points of Contact

Organization	Position	Name	DSN/Comm
USSOCOM POCs: SOAL-IIS-SDE SOAL-IIS-TACLAN SOIO-CM SOIO-CM SOIO-IC-R	(b)(3) 10 USC 130b, (b)(6)		
USASOC			
AFSOC			
NAVSPECWARCOM			

CAPABILITIES PRODUCTION DOCUMENT
FOR
SPECIAL OPERATIONS FORCES

TACTICAL LOCAL AREA NETWORK
(TACLAN)

27 January 2003

1. **Capability Discussion**. This document is a Capabilities Production Document (CPD) addendum to the existing C4IAS ORD and comes under the direction of the Special Operations Information Enterprise (SIE) Capstone Requirements Document (CRD). This CPD provides the operational performance parameters for the United States Special Operations Command (USSOCOM) Tactical Local Area Network (TACLAN) Program. TACLAN is the tactical equivalent of our Special Operations Forces (SOF) garrison automation networks. It provides the automation infrastructure and common-user applications to interconnect deployed SOF headquarters, main operating locations, tactical teams and liaison elements. Numerous joint, service, and SOF deployed automation programs/efforts rely on TACLAN to gain connectivity into the Global Information Grid (GIG). TACLAN consolidates numerous deployed SOF automation efforts into a consolidated infrastructure program consisting of hardware and common-user software applications that comply with the current Joint Technical Architecture (JTA) and the USSOCOM CIBL. For example, TACLAN captures and integrates deployed automation infrastructure efforts from SCAMPI (not an acronym) SOF Tactical Assured Connectivity System (SOFTACS), Joint Base Station (JBS), Special Operations Command Research, Analysis, Threat, and Evaluation System–Deployable (SOCRATES-D), Psychological Operations Broadcast System (POBS), Special Operations Forces-Intelligence Vehicle – Migration (SOF-IV (M)), Special Operations Tactical Video System (SOTVS), SOF radio programs, Special Operations Mission Planning Environment (SOMPE), and other mission planning programs. TACLAN is an enabler of USSOCOM Transformation goal. The goal is that SOF remain relevant and useful members of the joint team while maintaining the readiness required to shape and respond to the world today. Now and in the future, SOF must to be a full-spectrum, multi-mission force, capable of conducting strategic operations in tactical environments, while continuing to operate effectively in joint, combined, and interagency frameworks. TACLAN supports USSOCOM's goals via the Defense Planning Guidance (DPG) operational goal of Leveraging information technology and innovative concepts to develop an interoperable, joint C4ISR architecture and capability that includes a tailorable joint operational picture. According to the DPG, Network-Centric Warfare (NCW) is the cornerstone of transformation. Network-Centric Warfare is a broad class of approaches to military operations that are enabled by the networking of the force. The tenets of NCW are: a robust networked force improves information sharing; information sharing enhances the quality of information and shared situational awareness; shared situational awareness enables collaboration and self-synchronization and enhances sustainability and speed of command; these, in turn, dramatically increase mission effectiveness. TACLAN supports all of the tenets of NCW. Additionally, TACLAN supports the Quadrennial Defense Review (QDR),

September 30, 2001, pillar of strengthening joint operations through standing joint task force headquarters, improved joint command and control, joint training and an expanded joint forces presence policy

a. Capability Gap. . Current deployed SOF automation systems and networks have limited interoperability and functionality. Existing systems do not provide the needed automation systems or services necessary to support a deployed SOF Headquarters. This results in the deployment of larger numbers of personnel and equipment to perform the operational base functions, or, in some extreme cases, SOF elements have no automation support and rely on limited voice communications for mission planning and execution. Additionally, SOF units field various types of laptop computers and other hardware to perform similar functions, significantly complicating operational support and maintenance tasks. Multiple, stove-piped automation acquisition efforts negatively affect the USSOCOM Program Objective Memorandum (POM) build process, preventing senior leaders from making objective, fact-based funding decisions to provide a common SOF infrastructure and enhance SOF C4I interoperability.

b. SOF Mission Area. A TACLAN system and its components will serve as a force multiplier and critical contributor to information flow in support of SOF missions. This capability requirement also supports the following core tasks defined in USSOCOM message 01 05 202013Z MAY 03.

Core Tasks:

(1) Unconventional Warfare (UW)
(2) Foreign Internal Defense (FID)
(3) Direct Action (DA)
(4) Special Reconnaissance (SR)
(5) Counterterrorism (CT)
(6) Counterproliferation of Weapons of Mass Destruction (CP)
(7) Psychological Operations (PSYOP)
(8) Information Operations (IO)
(9) Civil Affairs Operations (CAO).

c. Spectrum of SOF Operations and Operating Environment. SOF operates across the warfare spectrum of nominal peace to full-scale war. SOF operates globally in a variety of difficult environments to include maritime, desert, jungle, mountains, and temperate forest and plain. Current trends indicate more future operations in an urban environment. Urban warfare tends to negate the traditional U.S. military's superiority in firepower and mobility, making SOF more suited than conventional forces to operate in this environment. Urban terrain will continue to provide leverages to potential adversaries who wish to combat U.S. forces asymmetrically and asynchronously. High tech weaponry and sensors enable SOF forces to operate effectively in urban areas. SOF can emplace sensors, provide intelligence (overt, covert or clandestine) collection, and provide target acquisition in the highly restrictive terrain of the urban environment. Through these methods, SOF can achieve strategic results unattainable by a larger conventional force. SOF provides the Theater Combatant Commanders with a full spectrum precision strike/reconnaissance force, and capitalizes on its mastery of the

asymmetric and asynchronous approaches to urban warfare. The TACLAN system will be employed throughout the full spectrum of USSOCOM missions, globally and in all weather conditions.

d. TACLAN Infrastructure. TACLAN provides a common deployed network infrastructure to support operations planning and reporting, orders dissemination and force execution, readiness and unit status monitoring, mission planning and analysis, mission rehearsal and execution, intelligence analysis and reporting, personnel support, health surveillance, and logistics planning and tracking. It includes the routers, hubs, switches, servers (file, mail, and proxy), network management and information assurance tools, printers, scanners, cabling, common-user and special-purpose (i.e., mission planning, imagery, etc) workstations to interconnect deployed automation customers. It also supports remote computing services to interconnect liaison elements and tactical teams to the main network, to include the fielding of automation devices (i.e., Field Computing Devices (FCDs)) for tactical teams. Currently, the FCD is a ruggedized laptop (threshold), eventually it will be centered around a core computer with a family of shells that can be selected based on the mission (objective). The FCD is a system that is portable, hand-held, fits into a Battle Dress Uniform (BDU)/Desert Camouflage Uniform (DCU) pocket (objective), and weighs no more than 5 pounds with the battery pack. Radio remote capabilities purchased under TACLAN will only include required network interface devices/software, with radio systems procured via other SOF and Service programs. FCD Threshold and Objective values are listed at Appendix F.

e. TACLAN Relationship to C4IAS. TACLAN is the deployed equivalent of USSOCOM garrison automation programs such as C4IAS. The Joint Mission Needs Statement (MNS) for USSOCOM C4IAS, approved on 22 Sep 97, provides the operational need for the development of TACLAN. The C4IAS MNS specifically addresses the need to extend the garrison system to deployed SOF locations. The C4IAS is a family of LANs and selected applications interfaced to various communications systems to form a wide area network connecting geographically dispersed garrison sites and is comprised of the following:

USSOCOM Command Local Area Network (LAN)
Special Operations Command Research, Analysis, Threat, and Evaluation System (SOCRATES)
Army Special Operations Command Network (ASOCNET)
Naval Special Warfare Command (NAVSPECWARCOM) LAN
Air Force LAN (AFLAN)
Command Planning Data Base (CPDB)
SOF Logistics and Acquisition Management System (SLAMS) (Army)
SLAMS (Air Force)
Special Tactics Network (STN)

Headquarters USSOCOM manages the C4IAS program. The system provides interfaces to external networks, such as SCAMPI, the Defense Information Systems Network (DISN), and the GIG.

f. Timeframe. SOF is actively involved in the War on Terrorism and has a requirement for a deployable network package for access into the NIPR, SIPR, and SCI clouds. This increment of TACLAN systems is envisioned as an evolutionary effort to provide a modular system capabilities integrated within the existing USSOCOM C4ISR architecture. Follow-on systems will reduce the footprint, enhance the interoperability, provide better MLS solutions, and introduce emerging technology as new capabilities reach maturity for practical employment. New capabilities will be introduced through Evolutionary Technology Insertion upgrades.

g. Architecture. TACLAN must be interoperable with existing C4I systems and employ an adaptable, open system architecture design to ensure compatibility and interoperability with future C4I developments. TACLAN will conform to the current and future JTA standards while emphasizing current COTS/GOTS technology to minimize integration and engineering costs and take advantage of the latest automation technologies. TACLAN is envisioned to be modular in design and a scalable suite of computer network equipment and workstations to permit maximum flexibility depending on the specific mission needs. It's developmental and acquisition strategy must enable fielding of new technologies as they become available to take advantage of improvements in automation support, evolving future systems, and architectures such as Joint Tactical Radio System (JTRS), Joint Operational Architecture (JOA), and Mission Information Management Architecture (MIM). The lifecycle support cost of the system will be minimized through commonality of hardware and software with other SOF Information Technology (IT) systems. TACLAN will support rapid deployments worldwide. A complete description of the anticipated operational and support concepts can be found in the TACLAN Concept of Operations (CONOPS) document.

2. Analysis Summary. A number of alternatives to a full and open competition to satisfy the TACLAN requirements were considered. These alternatives considered sole source acquisition of the USMC Tactical Data Network (TDN), the U.S. Air Force Theater Deployable Communications (TDC), the Joint Communications Support Element's (JCSE) TACLAN, or expansion of the SOF-IV (M) Program. A Market Investigation (MI) was performed in August 2000 to determine the feasibility of using Commercial Off-the-Shelf (COTS) / Non-Developmental Item (NDI) equipment to meet the ORD requirements. The MI results verified that there was sufficient technology maturity in the commercial IT/networking industry to proceed with a COTS / NDI strategy. It was determined that the ORD requirements could be satisfied through the use of COTS / NDI equipment, with incremental ETI block upgrades as technology matured. Specific details are contained in the TACLAN Market Investigation, dated August 2000. TACLAN will be acquired as a DOD 5000 ACAT III Program. The Low Rate of Initial Production (LRIP) materiel solution will be an integration of COTS / NDI equipment into ruggedized transit cases. The DPM will periodically perform additional MIs, as necessary, during subsequent block upgrade phases of the program in accordance with the TACLAN Migration Plan. The initial acquisition strategy facilitated maximum use of SOF resources by integrating the SOFTACS DLANs, SOCRATES Communications Interface Units (CIU), and SOF-IV (M). Due to the urgent and compelling need to field the Urgent Deployment Acquisition (UDA)

systems in support of Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF), SOAL awarded a contract to SPAWAR Systems Center – Charleston (SSC-C) for the DERF and supplemental TACLAN systems. SSC-C was also the integration contractor for the legacy DLAN systems. Given the history of SSC-C involvement with the DERF and legacy components of TACLAN, a competitive acquisition is not anticipated for the LRIP phase. Competition will be addressed in subsequent phases of the TACLAN program.

3. Concept of Operations Summary. TACLAN is the tactical equivalent of the SOF C4I Automation System (C4IAS) and a critical part of the SOF Information Enterprise (SIE). It will interconnect deployed SOF elements from the smallest team to a Joint Special Operations Task Force (JSOTF) headquarters with seamless, interoperable networks to share information, facilitate responsive knowledge based decisions, and provide an interface between the SOF Warfighter and the GIG. The TACLAN system and its components will serve as a force multiplier and enable information flow to assist in Command and Control (C2), intelligence, decision-making assistance, mission analysis, planning, health surveillance and execution support of all nine core tasks (ref para 1.b) that are the basis of SOF missions. TACLAN is envisioned to be a modular, scalable suite of computer network equipment and workstations providing similar functionality to the garrison suites. The TACLAN development effort will integrate current and future USSOCOM tactical automated information systems into an efficient, deployable information management system supporting the interchange of knowledge among commanders, operators, and support personnel. TACLAN supports a wide range of functions including command and control, intelligence analysis and reporting, office automation, decision-making assistance, mission analysis, planning, rehearsal and execution support. TACLAN's primary goal is to provide tactical automation connectivity with flexible interfaces to communications, databases, and mission applications that will collectively provide an equivalent of the garrison base architecture to deployed units and remote operators. Figure B-2 shows TACLAN's functionality using existing transmission systems to gain access to worldwide networks and existing mission applications to perform required functions. The mission applications listed under deployed users are just a sampling of the hundreds of application tools employed by deployed SOF units. TACLAN supports a wide range of functions for deployed SOF including Command and Control (C2), office automation, decision-making assistance, mission analysis, planning, health surveillance and execution support. The system will interface with remote servers and mission applications that provide intelligence, operations, administration, psychological operations (PSYOP), civil affairs (CA), medical, and logistics functionality. It interfaces with a mix of transmission systems available and programmed for SOF deployed forces to include tri/quad-band multi-channel satellite systems, high frequency (HF) radio, ultra high frequency (UHF) satellite, and Global Broadcast Services (GBS). The overall TACLAN effort supports the timely exchange of information between deployed and garrison SOF headquarters, main SOF operating locations, liaison elements (e.g., Special Operations Liaison Element (SOLE) and Special Operations Command and Control Element (SOCCE)), Operational Control Element (OCE), and tactical teams, and also facilitates liaison/coordination with Regional Combatant Commands (RCC), Services, Department of Defense (DOD) and Other Government Agencies concerning SOF operational

support (Figure B-3). As a JSOTF or subordinate SOF Headquarters operation progresses, the deployment scale and footprint may change from, initially small, perhaps larger in the mid-stages of an operation, and then shrinking during the redeployment phase. TACLAN will be scalable to accommodate easy network resizing to meet mission requirements. Through interfaces with worldwide communications networks such as SCAMPI (not an acronym), Non-secure Internet Protocol Router NETwork (NIPRNET), SECRET Internet Protocol Router NETwork (SIPRNET), and Joint Worldwide Intelligence Communications System (JWICS), TACLAN shall provide deployed SOF C2 nodes, staff elements and operators with multi-level information exchange to units/organizations/ agencies around the globe.

4. Threat Summary. Computer systems and automated networks that support SOF operations across the tactical, strategic, and sustaining base environments are critical to effective force management and mission success. The threat to a TACLAN is genuine, multifaceted, and growing. It comes primarily from individuals and groups both foreign and domestic. Adversaries recognize our civilian and military reliance on advanced information technologies and systems, and understand that information superiority provides the United States with unique advantages. Accordingly, potential foes are expected to pursue Information Operations (IO) to counter US military superiority. The primary tactical threat to TACLAN comes from IO. Intelligence indicates that offensive IO, such as Computer Network Operations (CNO) (Computer Network Exploitation [CNE] and Computer Network Attack [CNA]), Electronic Warfare (EW) (Electromagnetic Attack and Electronic Warfare Support, and physical destruction due to Electromagnetic Pulse [EMP]), and cyber-terrorism constitute the major threats to TACLAN and the communication systems on which it operates. This can include interception, exploitation, and degradation of commercial and military communication links or the signal environment by terrorist groups or foreign intelligence services. TACLAN will be a likely target through direct or indirect attacks to the system; network infrastructure; and Service, Agency, and Joint-provided data sources. Most of these threats are addressed in published DIA-validated documents. These include:

- *Information Operations Threat Capabilities Assessment*, DI-1577-12-03, July 2003, (S/NF), *Automated Information Systems Threat Environment Description (TED) (U),*
- National Air Intelligence Center (NAIC)-1574-0210-03, December 2002 (S/NF);
- *Military Satellite Communications (MILSATCOM) Systems Threat Assessment Report,* NAIC-1574-0367-03, February 2003 (S/NF);
- *Electronic Warfare Threat Environment Description (TED) (U)*, NAIC-1574-0731-01, Feb 01 (S/NF); and
- *Chemical and Biological Warfare Capstone Threat Assessment (U),* DI-1650-83-02, February 2002 (S//NF/X1).

The following documents provide additional information:

- *Information Operations Threat to the Defense Information Systems Network (DISN)(U)*, Defense Intelligence Agency (DIA)-2710-6-01, March 2001 (U);

- *Information Operations Threat to the Military Use of Commercial Satellite Communications (U)*, DI 2710-25-01, February 2001 (U);
- *A National Intelligence Estimate on the Cyber Threat to the U.S, National Intelligence Estimate (NIE) 2000-16-I*, December 2000; and
- *Worldwide Threats to Network Centric Warfare (U), Office of Naval Intelligence (ONI)-1573-002-02*, October 2001 (S/NF).

The IO threat continues to spread worldwide, with more mature technologies and more sophisticated tools being developed continuously. However, the level of threat varies widely from adversary to adversary. Most opponents currently lack the capability to fully integrate all IO tools into a comprehensive attack, especially against a system such as TACLAN. However, DoD systems are regularly probed and scanned by foreign locations as a prerequisite to exploitation or attack in order to define network architectures and assess vulnerabilities.

CNO tactics can be used against the TACLAN computer systems, operating systems, and software applications. CNO threats include stealing passwords and data, inserting malicious code, denial of services, and data corruption, modification, and manipulation. Additionally, physical threats to TACLAN include the entire spectrum of direct and indirect fire weapons, WMD, environmental factors, chemical contamination, and lingering or transitory impacts on the electromagnetic environment.

5. Program Summary. The TACLAN concept originated in May 1998 when the PEO-IIS received a concept briefing and directed the Deputy Program Manager (DPM), SOF Intelligence Vehicle-Migration (SOF-IV (M)) to coordinate with the PM, C4IA and develop a consolidated recommendation for implementing a TACLAN program. SOIO was tasked to develop a TACLAN ORD, which was approved by the Special Operations Command Requirements Executive Board (SOCREB) in June 2001. It included a Basis of Issue Plan (BOIP) of 156 TACLAN suites. Since that time, additional responsibilities and manpower at the components and TSOCs have increased the BOIP to 167 TACLAN suites. In response to urgent and compelling operational needs, primarily providing support to Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF), 37 UDA, pre-production TACLAN suites were produced and fielded with DERF and Supplemental funding. All fielded pre-production TACLAN suites have been/will be incorporated into the TACLAN program baseline, in accordance with the TACLAN Migration Plan. The operational use of TACLAN helped refine and establish the hardware and software architectures. Additionally system-wide fixes and improvements were identified and implemented by the Life Cycle System Manager (LCSM) during user assessments and feedback. These are incorporated as part of the system baseline.

The TACLAN Acquisition Approach is based on an evolutionary, event-driven, acquisition with a series of planned incremental upgrades. It is composed of the following three (3) phases:

- **Phase I. Milestone C, LRIP Approval Decision.** Phase I began when Milestone C, LRIP approval was received. Phase I goals were to acquire and test two (2) Low-Rate Initial Production (LRIP) systems; initiate implementation of the TACLAN migration plan to address legacy system compliance with the current hardware and software baselines; conduct a detailed CPI analysis to determine requirements for preparation of a PPP and/or SCG; and refine the TACLAN acquisition strategy. $1.1M of FY02 procurement funds on the SSC-C contract was used to integrate and test two (2) LRIP units. LRIP and Supplemental TACLAN hardware and software configurations constituted the system baseline, incorporating system fixes and improvements identified during previous user assessments and from user feedback as the result of operational use. The software baseline was integrated and tested using the approved SIF integration process. Production Qualification Testing (PQT) was performed to verify the LRIP configurations comply with TACLAN technical performance parameters. Tailored Operational Testing (TOT) was performed to verify the operational effectiveness and suitability parameters of TACLAN. This tailored operational test and evaluation (OT&E) consisted of collecting effectiveness and suitability data during TACLAN New Equipment Training (NET) and fielding, using the results of operational assessments previously conducted on TACLAN supplemental systems, after action reports, and user feedback. Data was collected from user personnel that operated and maintained TACLAN systems during operational missions and training exercises. Follow-on Operational Testing (FOT) will be performed as necessary. Pre-production TACLAN suites will be modified to bring those systems in compliance with the current baseline.

- **Phase II. Milestone C, Full Rate Production (FRP).** Phase II will commence upon approval for Milestone C – FRP. The goals of Phase II are to begin FRP of the approved program baseline and complete the migration of legacy systems. Production quantities are based upon funding availability. An agreement between PEO-IIS, Assessment Directors, and SOIO to develop complete program cost estimates, based upon SOIO final requirements determination and a cost-to-performance tradeoff analysis, will be executed during the FY04-09 POM. This will serve as an incremental strategy to build on program accomplishments and expand TACLAN fielding to the Components.

- **Phase III. Milestone C, Sustainment and ETI Enhancement.** Program emphasis will shift to ensure consistent sustainment of TACLAN's operational suitability, including continued ETI enhancements, throughout the program's life cycle. Primary efforts will focus on ETI Block upgrades, technology infusion, and implementation of ORD objective requirements.

6. System Capabilities Required for the Current Increment. TACLAN requirements are delineated as threshold or objective, with three (3) threshold requirements designated as the system's Key Performance Parameters (KPP). There are an additional twelve (12) threshold requirements identified as System Core Characteristics and Capabilities. The following subparagraphs define KPPs and Core System Characteristics and Capabilities. TACLAN must operate as specified below:

a. Multiple Levels of Security (KPP). TACLAN must provide the user with the ability to operate at different security levels (unclassified, Secret, and Sensitive Compartmented Information (SCI)) (Threshold), Secret to include Focal Point, and releasable to coalition (Objective). This may be achieved through the use of multi-LAN capabilities that operate system high on networks at various security levels. TACLAN will have the capability to transport data utilizing National Security Agency (NSA) endorsed security protection mechanisms, in accordance with USSOCOM, DOD, and Intelligence Community (IC) security policies, at different security classification levels without any likelihood of intermixing or corruption of data (Threshold). TACLAN will provide an MLS capability where one workstation can sequentially process and access several levels of security, using removable media and operating systems (Threshold). Connection to any network, classified or not, must be architecturally consistent with the security level of that network (Threshold). TACLAN will provide a Multi-level Security (MLS) capability where one workstation can process and access several levels of security (Objective).

b. Scalability and Modularity (KPP). The TACLAN network will be configured into standardized configurations based on organization and echelon level (Threshold). Network packages will be modular and permit flexible addition of capabilities to live networks with minimum interruption in service (Threshold). TACLAN equipment will be packaged into transit cased modules based on equipment functionality to enable operators to deploy tailored network configurations (Threshold).

c. Interoperability (KPP). TACLAN will comply with the established GIG policy and applicable JTA standards (Threshold). All top-level IERs will be satisfied to the standards specified in the threshold (T) and Objective (O) values in Table D-1. This includes commercial-to-military information transfer and transfer between U.S. and Combined forces (Threshold). System will interoperate with worldwide information networks including strategic networks, worldwide theater systems/information networks and deployed theater LANs, and all SOF information and intelligence networks (Threshold). System must be interoperable with SOFTACS, SOF Deployable Node (SDN), Theater Deployable Communications (TDC) and the Public Switched Telephone Network (PSTN) (Threshold). System must interoperate with NIPRNET, SIPRNET, USSOCOM C4IAS, and JWICS (Threshold). System will interface with Tactical Packet Network (TPN) (Threshold). System will interoperate with Defense Message System (DMS) or equivalent, Army Battle Command System (ABCS), Theater Battle Management Core Systems (TBMCS), POBS, Joint Deployable Intelligence Support System (JDISS), Global Command & Control System (GCCS), and Global Combat Support System (GCSS), Portable Intelligence Collection and Relay Capability (PICRC), Product Development Workstation (PDW) – Light, and Theater Medical Information System (TMIP) (Threshold). System will interface with Warfighter Information Network – Tactical (WIN-T) when available (Objective). System will operate with Ethernet, Gigabit-Ethernet, Asynchronous Transfer Mode (ATM) (Objective), or ISDN and Euro ISDN when required (Threshold).

d. Transportability. TACLAN must facilitate worldwide transportation in transit cases, as restrained cargo, in currently fielded and commercial land/sea/air mobility platforms (Threshold). Transit cases/packaging must protect TACLAN equipment from extreme temperatures (low of –50° F and a high of +160° F), wind, rain, snow and ice, sand, dust, dirt, mud, humidity, saltwater corrosion, and the effects of vibration and altitude and still operate within the temperature parameters described in paragraph 14b (Threshold). Ruggedized, shock absorbent transit cases will provide protection of all system components during in-transit mobility and storage (Threshold). Workstations and network components will be transported in ruggedized transit cases with no more than two-man lift restrictions (Threshold). For TACLAN network configurations of 10 workstations (or less), TACLAN equipment will be packaged into transit cases that can be carried by one person and fit into the overhead compartment of a commercial airliner (Objective). The smaller transit cases will facilitate the rapid, low signature deployment of smaller network packages supporting tactical teams and/or small-scale deployments. Transit cases will allow for connection of tie down devices for either vehicular and/or palletized mode for air, sea, and rail transport (Threshold). System, not including supporting communications equipment, will be capable of transport in palletized transit case modes on all SOF fixed wing aircraft, strategic airlift (e.g., C5, C17), and floor load on SOF rotary wing aircraft (Threshold).

e. Reliability. Reliability will be considered up front during the initial selection of system components. USSOCOM/SOOP will initiate a reliability growth plan that starts with the inception of TACLAN and the TACLAN Program Manager will manage reliability through component replacement and component improvement over the life of the program. TACLAN will provide operational reliability by the development and publishing of a Reliability and Maintainability Rationale Report (RRR) (Threshold). The system will also have non-volatile storage with backup/restoral capabilities (Threshold). System's storage process shall not alter stored data in a manner that compromises the integrity of the data/information (Threshold). System shall provide visibility of storage infrastructure to efficiently manage storage capacity and provide the capability to remove/discard stored data as required (Threshold). System's data shall be stored in a manner that facilitates distribution IAW processing and transport needs and supports the rapid retrieval of information by the user (Threshold). System's data shall be stored in a manner that assures the required access to and use of all needed data, and in a way that prevents the loss of stored data from physical threats such as fire, water damage, information operation threats, and Electromagnetic Pulse (EMP) as appropriate to the information being stored (Threshold). System's data that is no longer required shall be disposed of effectively and efficiently, so that the storage space that was used by the disposed data can be used for the storage of new data without the user having to do any additional actions once the decision to dispose has been made (Threshold). System's data shall be retained in a manner that meets all mission and regulatory guidance and is transparent to the user (Threshold). TACLAN network capacity will allow a minimum surge increase of 30% in network use without impacting mission performance (Threshold). Sufficient spares will be provided so the time to restore workstations/FCDs will be no more than 60 minutes (this includes administrative

logistics down time (ALDT)) (Threshold). Spares for network components will be provided so the time to restore will be no more than 30 minutes (Threshold).

f. Network Capacity. TACLAN will provide automation capabilities and network services in worldwide field conditions equivalent to garrison LAN operations (Threshold). TACLAN must support the user's operational requirement to rapidly and reliably exchange data/information. TACLAN will maximize onsite bandwidth for the greatest throughput. This will be accomplished by employing sound information management practices, file compression, size restrictions, etc to pass bandwidth intensive imagery, video, sensor feeds and sensor broadcasts on demand. How rapidly the network transports information offsite is dependent on transmission speed and network availability. Timeliness in Table 1 is assuming there are no external restrictions on transmission speed and network availability. Table 1, Network Capacity and Timeliness, identifies the type, size, and delivery rates of that data/information.

Type of Data	Size	Timeliness
Unit readiness and status reporting	< 500 KB	10 seconds (Threshold) 3 seconds (Objective)
Intelligence analysis and reporting	< 10 MB	1 minute (Threshold) 30 seconds (Objective)
Operations planning and reporting	< 1 MB	30 seconds (Threshold) 15 seconds (Objective)
MPR&E support	< 500 KB	10 seconds (Threshold) 3 seconds (Objective)
Orders dissemination and force execution	<500 KB	10 seconds (Threshold) 3 seconds (Objective)
Weather data	< 5 MB	1 minute (Threshold) 30 seconds (Objective)
Geographic data	< 5 MB	1 minute (Threshold) 30 seconds (Objective)
Mapping data	< 10 MB	1 minute (Threshold) 30 seconds (Objective)
Imagery data	< 10 MB	1 minute (Threshold) 30 seconds (Objective)
Logistics planning, personnel administration, and other support function	< 500 KB	10 seconds (Threshold) 3 seconds (Objective)

Table 1 Network Capacity and Timeliness of Service

g. Deployability. Server configuration will be accomplished prior to deployment. Two operators will be able to complete physical system setup of a ten-workstation network within one hour (Threshold); a 100-workstation network within 48 hours; and a 300-workstation network within 72 hours(Systems are not currently issued with 100/300 workstation capacity, therefore no testing is required). Two operators will be able to complete physical system setup of a ten-workstation network within 30 minutes; a 100-workstation network within 24 hours; and a 300-workstation network within 48 hours

(Objective). Two operators will be able to redeploy a ten-workstation network, including full system disassembly and complete network degradation, within 30 minutes (Threshold); a 100-workstation network within 24 hours; and a 300-workstation network within 36 hours (Systems are not currently issued with 100/300 workstation capacity, therefore no testing is required). Two operators will be able to redeploy a ten-workstation network, including full system disassembly and complete network degradation, within 20 minutes; a 100-workstation network within 12 hours; and a 300-workstation network within 24 hours (Objective). Setup/tear down times may be longer at extreme temperatures and/or within a Nuclear Biological Chemical (NBC) environment (Threshold).

h. Network Access. TACLAN will rely on existing wide area network transmission systems to provide connectivity into the GIG including SOF, DOD, and other networks. TACLAN will interface with communications from joint to unit level, deployed units/elements, the Joint Task Force (JTF), other Services, and CONUS/Theater C2 nodes/centers (Threshold). System will provide interface for U.S. military, joint, commercial, Host Nation/Coalition networks (Objective). A Remote Access Subscriber interface (RAS) will augment TACLAN and provide scalability and capability to provide service to remote users. The RAS will provide multiple loop connections (multiple users able to connect at once) (Threshold). The RAS will support at least one secure and one non-secure LAN (Threshold).

j. System Power. TACLAN will use available military or commercial power in support of worldwide operations at deployed locations, bare bases, and on Host Nation installations (Threshold). The system will provide the capability to use power variants based on worldwide availability, 90 - 250 VAC at 43 - 63 Hz (Threshold). System will provide both visual and non-visual (audio) indications when primary power is lost (Threshold). System power equipment will include Uninterrupted Power Source (UPS) with back up power capacity to operate the system for a minimum of 15 minutes (Threshold). This will allow for a controlled shutdown of systems. The minimum requirement is for the servers, routers, and PIX firewalls to be connected to the UPS. Other items may be connected but UPS time degradation will be allowed for anything connected above the minimum requirement. UPS will be capable of over voltage protection, lightning/surge protection, and line conditioning (Threshold). System power equipment will include UPS with back up power capacity to operate the system for a minimum of 24 hours (Objective).

j. Technological Insertion. To effectively keep pace with advances in technology that have the potential to render existing systems obsolete shortly following acquisition, TACLAN will provide for technology insertion and capacity growth capabilities that will interoperate with related, newly developed, JTA approved systems (Threshold). Technology insertion will follow USSOCOM CIBL guidelines. The USSOCOM Engineering Change Request (ECR) process will be used by all USSOCOM elements including Components and TSOCs to propose configuration changes and evolutionary upgrades that do not change TACLAN's operational requirement. The TACLAN Program Manager, in coordination with the TACLAN User Representative, will identify

and propose block upgrades as technology matures and/or propose replacements should the TACLAN no longer satisfy user requirements. Approved hardware and software upgrades will be designed and executed to ensure minimal impact on users.

k. Standardization. TACLAN will comply with the following standards and policies:

JTA standards, procedures and policies (Threshold)
International Standards Organization (ISO) Open System Interconnection (OSI) architecture (Threshold)
Electromagnetic Compatibility (EMC) commercial design standards (Threshold)
DISA, DIA, and DODIIS standards (Threshold)
JTA Defense Information Infrastructure (DII)/Common Operating Environment (COE) level 6 (Threshold)
DII/COE level 8 (Objective)
DMS protocols and procedures (Threshold)
National Imagery Transfer Format Standards (NITFS) (Threshold)
Global Information Grid Capstone Requirements Document compliance checklist
USSOCOM CIBL (Threshold)

l. Semantic Tagging. GIG CRD requirement for semantic tagging of information to the CPD: "All of a system's data that will be exchanged, or has the potential to be exchanged, shall be tagged in accordance with the current JTA standard for tagged data items (e.g., Extensible Markup Language [XML], the current JTA standard), and tags shall be registered in accordance with the DOD XML Registry and Clearinghouse policy and implementation plan (Threshold, KPP). System's data being stored shall include its classification and releasability criteria within the semantic tag or associated schema (Threshold).

m. Network Management. The TACLAN Network Management System (NMS) must manage network performance through monitoring designated Internet Protocol (IP) components associated with TACLAN and provide statistical, graphical, and analytical tools to support performance management (Threshold). The TACLAN NMS will provide an integrated network management capability providing an automated means to plan, initialize, test, and manage the deployed network, both locally and remotely (Threshold). Systems shall have an automated NM capability to obtain status of networks and associated assets in near real time 99% (Threshold, KPP) and 99.9% (Objective, KPP) of the time. TACLAN will use software that will perform automated network performance analysis and automated fault management to include problem detection, fault isolation and diagnosis, problem tracking until corrective actions are completed, and historical archiving (Threshold). Systems shall have a NM capability that leverages existing and evolving technologies and has the ability to perform remote network device configuration/reconfiguration of objects that have existing DOD JTA management capabilities (Threshold). To accornplish GIG end-to-end situational awareness, systems shall have the NM capability of automatically generating and providing an integrated/correlated presentation of networks and all associated network assets (Threshold). System will maintain an audit trail including automatic discovery of

network devices, automatic population of network management databases, and automatic reporting of network status (Threshold). All transport elements (e.g., switches, routers, etc.) shall be capable of providing status changes to network management devices by means of an automated capability in near real time 99% (Threshold, KPP) and 99.9% (Objective, KPP) of the time. TACLAN will be compatible with the Joint Network Management System (JNMS) when available (Objective).

n. Key Performance Parameters:

	Key Performance Parameters	Threshold Requirements	Objective Requirements
1.0	**Multiple levels of Security**	**Manage networks and operate on networks at various security levels. Removable storage media required to meet security directives.**	**Integrate with JNMS and integrate enterprise information across multiple security levels IAW NSA approved procedures**
1.1	Support Unclassified, collateral, and SCI processing	Separate LANs accessed with the same workstation via removable media and switches.	Capable of accessing multiple networks with same workstation. JNMS
1.2	Support SPECAT and releasable to coalition processing	N/A	Capable of accessing multiple networks with same workstation. JNMS
1.3	Data transport between different classification levels	Transport data using NSA endorsed security protection measures at different classification levels without intermixing or corruption	Automatic multi-level security capability
1.4	Architecture consistency	Connection to any network must be architecturally consistent with security level of that network.	Same as Threshold
2.0	**Scalability and Modularity**	**Scalable into standardized configurations based on organization and echelon level**	**Same as Threshold**
2.1	Introduction of additional capabilities	Permit additional capabilities into a "live" network	Same as Threshold
2.2	Packaging	Equipment will be packaged into transit cased modules based on functionality to enable users to deploy tailored network configurations	Same as Threshold
3.0	**Interoperability All top-level IERs will be satisfied to the standards specified in the threshold (T) and Objective (O) values**	**100% of top-level IERs designated critical**	100% of all top-level IERs
3.1	Interoperate with Strategic networks	Through DISN gateway (STEP sites)	Through DISN gateway (DOD Teleport)
3.2	Interoperate with worldwide information networks	Through DISN gateway (STEP sites)	Interface with allied and coalition networks
3.3	Interface with deployed Theater LANs	Ethernet Networks (802.3), ATM, or equivalent capability	TBD Wide Area Protocol

	Key Performance Parameters	Threshold Requirements	Objective Requirements
3.4	Connect with hardware used in SCAMPI, MSE, and TRI-TAC	Draw JWICS, SIPRNET, NIPRNET services.	TBD as developed (see "technology insertion")
3.5	Interoperate with SOF and Service transmission systems	SOFTACS, Deployed SCAMPI, TDC, PSTN (remote dial-in) and ISDN.	TBD
3.6	Interface with NIPRNET, SIPRNET, USSOCOM C4IAS, JWICS	Through DISN gateway (STEP sites), SCAMPI	Through DISN gateway (DOD Teleport)
3.7	Interface with JWICS	NRT ELINT, SIGINT, and IMINT data; archived IMINT data; video	TBD
3.8	Interoperate with tactical networks	Tactical Packet Network (TPN), SMRS, JBS/RIS, and MBMMR radios.	Warfighter Information Network – Terrestrial (WIN-T)
3.9	Interface with DMS, TBMCS, JDISS, GCCS, GCSS, PICRC, PDW-Light	Through DISN gateway (STEP sites), SCAMPI	TBD
3.10	Interface with Ethernet, Gigabit Ethernet, ATM and ISDN	EuroISDN, Ethernet	Gigabit Ethernet, ATM, ISDN, Fiber

Table 2 Key Performance Parameter

o. Additional Attributes Correlation Requirements:

	Core System Characteristics and Capabilities	Threshold Requirements	Objective Requirements
1.0	**Environmental**	**Deploy and operate in field environments worldwide**	**Same as Threshold**
1.1	Storage and transit.	TACLAN components must meet be able to operate after storage and transport within conditions of wind, rain, ice, snow, and dust and in temperatures of -50° F to +160° F	Same as Threshold
1.1	Operating temperatures	TACLAN equipment (consists of workstations and network components, it does not consist of any peripheral devices such as ; printers, scanners, projectors, etc.) must be able to operate under the following conditions: Internal operating conditions: +40° F to +90° F See note on 14b. FCD components must be able to operate between 40° F and +120° F	All TACLAN components operate between –20° F and +130° F

	Core System Characteristics and Capabilities	Threshold Requirements	Objective Requirements
2.0	**Transportability**	**Facilitate worldwide transportation in transit cases, as restrained cargo, in currently fielded/commercial land/sea/air mobility platforms**	**Same as Threshold**
2.1	Transit cases/packaging	Transit cases/packaging must resist conditions of temperature (Low = -50° degrees F, High = +160° degrees F), wind, rain, snow and ice, sand, dust, dirt, mud, humidity, saltwater corrosion, and the effects of vibration and altitude	Same as Threshold
2.2	Weight and volume	Weight of individual transit cases with removable wheels or casters will not exceed two-man portable capacity.	Network configurations of less than 10 will be packaged in transit cases not to exceed one-man lift and fit into the overhead compartment of a commercial airliner to facilitate small deployments and tactical teams.
2.3	Shelter requirements	None	TBD
2.4	Vehicle Prime Mover Requirement	None	TBD
2.5	Aircraft cargo	The system (not including communications equipment) will be transportable in either vehicular or palletized transit case component configurations on all SOF fixed wing aircraft, strategic airlift (C5, C17), and floor load on SOF rotary wing aircraft	TBD
2.6	Sealift and rail cargo	Transit cases will allow for proper connection of tie down devices for either vehicular and/or palletized mode sea and rail transport	TBD
3.0	**Reliability**	**Provide operational reliability through development and publishing RRR.**	**TBD**
3.1	Ensure reliability of data	Non-volatile storage with backup/restoral capabilities	TBD
3.2	Surge mission use will not impact system performance	Minimum surge increase of 30% in network use	TBD
3.3	Workstations/FCD Spares	Sufficient spares will be provided so time to restore will be no more than 60 minutes. FCDs will be spared at 10% to the component commands.	TBD
3.4	Network component Spares	Sufficient spares will be provided so time to restore will be no more than 30 minutes	TBD
4.0	**Network Capacity**	**Provide automation throughput capabilities and network services in worldwide field conditions comparable to garrison level functionality**	**TBD**
4.1	Unit readiness and status reporting (<500 KB)	All network classifications, 10 seconds	All network classifications 3 seconds

	Core System Characteristics and Capabilities	Threshold Requirements	Objective Requirements
4.2	Intelligence analysis and reporting (<10 MB)	All network classifications, 1 minute	All network classifications 30 seconds
4.3	Operations planning and reporting (<1 MB)	All network classifications, 30 seconds	All network classifications, 30 seconds
4.4	MPR&E support (< 500 KB)	All network classifications, 10 seconds	All network classifications, 3 seconds
4.5	Orders dissemination/force execution (< 500 KB)	All network classifications, 10 seconds	All network classifications, 3 seconds
4.6	Weather data (<5 MB)	All network classifications, 1 minute	All network classifications 30 seconds
4.7	Geographic data (<5 MB)	All network classifications, 1 minute	All network classifications 30 seconds
4.8	Mapping data (<10 MB)	All network classifications 1 minute	All network classifications 30 seconds
4.9	Imagery data (<10 MB)	All network classifications 1 minute	All network classifications 30 seconds
4.10	Logistics planning and tracking, personnel administration, medical, and other support functions (<500 KB)	All network classifications 10 seconds	All network classifications, 3 seconds
	Core System Characteristics and Capabilities	Threshold Requirements	Objective Requirements

	Core System Characteristics and Capabilities	Threshold Requirements	Objective Requirements
5.0	Deployability	Easily deployable workstation and network equipment	TBD
5.1	Perform timely system deployment and setup	Two operators will be able to complete physical system setup of a 10-workstation network within one hour; 100-workstation network within 48 hours; and 300-workstation network within 72 hours. (Servers will be configured prior to deployment).	Two operators will be able to complete physical system setup of a 10-workstation network within 30 minutes; 100-workstation network within 24 hours; and 300-workstation network within 48 hours. (Servers will be configured prior to deployment).
5.2	Perform timely system tear-down and redeployment	Two operators will be able to redeploy a 10-workstation network, including full system disassembly and complete network degradation, within 30 minutes; a 100-workstation network within 24 hours; and a 300-workstation network within 48 hours.	Two operators will be able to redeploy a 10-workstation network, including full system disassembly and complete network degradation, within 20 minutes; a 100-workstation network within 12 hours; and a 300-workstation network within 24 hours.
5.3	Extreme conditions	Setup and tear down times may be longer at extreme temperatures and/or in NBC environment	TBD
6.0	Network Access	Use existing wide area network interfaces from joint to unit level, deployed units/elements, the Joint Task Force (JTF), other Services, and CONUS/theater C2 nodes/centers	U.S. military (joint/combined), commercial, host nation, coalition networks
6.1	Remote access	The RAS will provide multiple connections for remote users	TBD
6.2	Remote access	The RAS will support at least one secure network and one non-secure network	TBD
7.0	System Power	Use power for worldwide operations at deployed locations, bare bases and on host nation installations	TBD
7.1	Provide capability to use power variants based on worldwide availability	Operate on all voltages from 90 - 250 VAC at 43 - 63 Hz.	TBD
7.2	System will provide both visual and non-visual (audio) indications when primary power is lost	System power equipment will include UPS with back up power capacity to operate the system for a minimum of 15 minutes	System power equipment will include UPS with back up power capacity to operate the system for a minimum of 24 hours
7.3	Equipment Protection	UPS will be capable of over voltage protection, lightening/surge protection, and line conditioning	Same as Threshold
7.4	Maintain critical information during power interruptions	System will retain router databases in non-volatile memory during power interruptions.	TBD
7.5	Peripheral equipment will include UPS and/or surge protection.	Provide protection from over voltage and lightening/surge protection	Provide capacity to operate system for a minimum of 24 hours

	Core System Characteristics and Capabilities	Threshold Requirements	Objective Requirements
8.0	Technological Insertion	Provide technology insertion and capacity growth capabilities to interoperate with related newly developed, JTA approved systems	TBD
9.0	Standardization	Architecture standards will comply with JTA security standards, procedures and policies	TBD
9.1	Architecture requirements	In accordance with (IAW) ISO OSI architecture standards	TBD
9.2	Design standards	IAW EMC commercial design standards	TBD
9.3	Comply with DODIIS standards	DIA DODIIS Instruction 2000	TBD
9.4	Architecture complies with JTA (Y2K and DII COE)	Y2K compliant and scalable to DII COE level 6	Scalable to DII COE level 8
9.5	Defense Message System (DMS)	Provide an interface to the DMS system and comply with DMS protocols and procedures	TBD
9.6	Imagery processing	IAW NITF standards	TBD
9.7	Hardware and software selection	IAW USSOCOM APL	Same as Threshold
10.0	Network Protection and Security	Use network security software that will provide strong identification, authentication, access control and auditing capabilities and integrity services utilizing a secure operating system. Network control functions will prohibit unauthorized access to restricted network and information, support security and system-monitoring capabilities, control database read/write capabilities, and provide log-on from anywhere in network.	Execute scalable integration with IA tools as they are developed to include voice and digital signatures, imprint identification, and identification and validation of secure protocols and improved system/network boundary guards. Integrate network security with JNMS.
10.1	Provide alert and monitor of abnormal network activity	IAW USSOCOM Manual 380.3 Information Assurance Program	JNMS
10.2	Support network intrusion protection	IAW USSOCOM Manual 380.3 Information Assurance Program	JNMS
10.3	Support integration of firewalls	IAW USSOCOM Manual 380.3 Information Assurance Program	JNMS
10.4	Provide protection from unauthorized tampering, access or updates	Provide automatic detection and alarm for network intrusion	None
10.5	Support integration of computer virus scanning software	IAW USSOCOM Manual 380.3 Information Assurance Program	JNMS
10.6	Support an integrated security management concept	IAW USSOCOM Manual 380.3 Information Assurance Program	Display regional Defense Information Operations (DIO) device status. Receive, process and display status and event information from all affiliated Information Assurance (IA) management systems (JNMS).

	Core System Characteristics and Capabilities	Threshold Requirements	Objective Requirements
10.7	Support system backup/restoral software	Provide automatic system backup/restoral	Same as Threshold
10.8	Incorporate link encryption that is fully interoperable with GIG and JTA security architectures	IAW USSOCOM Manual 380.3 Information Assurance Program	JNMS
10.9	Support system security capabilities	Maintain a consistent network security interface	JNMS
10.10	Provide user access control	Provide control of user access and permissions, user access time periods and user log-on authentication	TBD
10.11	Manage user-id and passwords for access	Limit access to single user-id/any system and single password/any system with log-in from anywhere in the network	Public Key Infrastructure (PKI)
11.0	Network Management	Use network management software that provides an automated means to plan, initialize, test, and manage the deployed network, both locally and remotely	Provide functional interface with higher-level network management systems, while avoiding duplication of status and services (JNMS)
11.1	Perform automated network performance analysis	Monitor designated components and provide statistical, graphical, and analytical tools	Interface with Information Dissemination Management (IDM) software applications (JNMS)
11.2	Support system monitoring capabilities	Automated means to plan, initialize, test, and manage the deployed network both locally and remotely	Interface with Information Dissemination Management (IDM) software applications (JNMS)
11.3	Perform automated fault management	Detect and isolate faults while ensuring rapid system recovery and reallocation of resources during expected denial of network services	Interface with Information Dissemination Management (IDM) software applications (JNMS)
11.4	Maintain a network audit trail	Automatically discover network devices, populate network management databases and automatically save/report network status	Interface with Information Dissemination Management (IDM) software applications (JNMS)

Table 3 Additional Attributes Correlation Matrix

7. **Family of System and System of System Synchronization**. This CPD drives a capability solution for a network system capable of interoperating on envisioned network architectures thus this CPD falls under the purview of the Global Information Grid CRD. This CPD drives capabilities that, in the long term, allow for continuous, tailored information to be disseminated with sufficient accuracy, to any SOF battlespace worldwide. It is imperative that transparent connectivity exists among multi-service systems and C2 assets. New generations of systems operating in the joint environment must offer similar and interoperable data formats, network characteristics, and performance characteristics. The TACLAN System will be a network node in the GIG. The TACLAN connectivity with the GIG and compliance with the GIG Architecture will provide the user interfaces necessary to access DoD, National Security, Intelligence

Community and other Government information enterprises. The GIG Bandwidth Expansion (GIG-BE) program directly impacts the ability of the TACLAN System to connect high bandwidth ISR and IC users to the terrestrial GIG backbone. The TACLAN System will connect to the GIG through DoD and commercial transport systems. See Appendix A for the CDD to GIG Capstone Requirements Document (CRD) crosswalk.

8. National Security System and Information Technology System (NSS and ITS) Supportability. Estimated bandwidth is listed in paragraph 6 f and in the Information Exchange Requirements Matrix (Table B-1) paragraph 4. Currently there is no requirement for Quality of Service (QoS) requirements or prioritization.

9. Intelligence Supportability.

a. General. TACLAN will provide intelligence COTS/GOTS applications in the following areas: collection, processing, production, and dissemination. The applications must provide the capabilities outlined below.

b. Collection. The intelligence functional area of collection "includes both the acquisition of information and the provision of this information to processing and/or production elements." (JCS Pub 2-0). The collection functional area includes collection operations management. As an objective capability, SOF intelligence requires an automated capability to manage and synchronize collection operations for collection assets that are organic, attached to, or supporting SOF forces. TACLAN workstations must provide for the automated capability to monitor and input tactical, theater, Service and national intelligence collection requirements in the following areas:

(1). Imagery Intelligence (IMINT). Provide for the automated capability to monitor national, theater and tactical imagery collection activities and submit imagery collection requirements.

(2). Signals Intelligence (SIGINT). Provide for the automated capability to monitor national, theater and tactical SIGINT collection activities and submit SIGINT collection requirements.

(3). Human Intelligence (HUMINT). Provide for the automated capability to monitor source data record/message traffic and directly interface with Defense Attaché Office (DAO) AIS. Additionally, provide for the capability to submit HUMINT requirements to collection activities.

(4). Health Surveillance (HS). Provide the automated capability to capture health, occupational, and environmental information at the point-of-exposure or care.

(5). Measurement and Signatures Intelligence (MASINT). Provide for the automated capability to monitor MASINT collection activities and submit MASINT collection requirements.

c. Processing. The intelligence functional area of processing "is the action of converting information to formats that can be readily used by intelligence personnel in the analysis and production of intelligence". (JCS Pub 2-0) SOF analysts require community wide interoperability to ensure the capability to process information from SOF, theater, Service, and national level intelligence and C2 AIS while deployed.

(1). Intelligence Fusion. As an objective capability, TACLAN workstations must provide the capability to conduct all-source (including Open Source Intelligence Information (OSINT)) and single source automated intelligence fusion/correlation to provide a timely, accurate and viable "common intelligence picture" of threat forces. The SOF intelligence analyst must be able to establish specific filters from the workstation for specific fusion/correlation capabilities. This threat driven fused situation display must be capable of being integrated into the Global Command and Control System (GCCS) "common operational picture."

(2). Record Message Handling. TACLAN workstations must provide for the automated processing and integration of unclassified, collateral, SCI and special category incoming and outgoing message traffic. SOF intelligence requires automated message receipt; routing and profiling; message generation, release and transmission; and the ability to query message databases utilizing keyword, date time group, subject, and other data field message entries for worldwide, SCI and GENSER messages. SOF intelligence requires on-line interfaces to Automatic Digital Network (AUTODIN) and Defense Special Security Communications System (DSSCS) message traffic, and to the Defense Message System (DMS) or equivalent (threshold). Access to newswire services is also required.

(3). Information Discovery and Retrieval. TACLAN workstations must provide the capability to conduct a rapid search of multiple data sources. As an objective capability, this will be done using a single logical search query. Data sources include both structured and unstructured databases, and web-based servers. Priority desired sources include general military intelligence (GMI) databases, automated message handling systems, and web-based servers such as INTELINK/INTELINK-S.

(4). Geospatial Information and Services (GI&S). TACLAN workstations must provide for automated access and capability to annotate/manipulate geospatial products. High-resolution digital terrain elevation data (DTED) at all levels is critical to SOF mission planning and rehearsal capabilities. TACLAN workstations must provide access to maps and charts now available on CD ROM/soft copy in vector format, with the capability to print to a color printer. Intelligence analysts also require automated tools to support topographic, hydrographic, oceanographic, and weather analysis.

(5). Imagery. SOF intelligence processing capabilities include image file, geospatial file, video retrieval and enhancements. Enhancements (or manipulations) of such files include image rotation, gray scaling, file format changing, brightness/contrast modifications and inversions. The processing of any given image may include some or all of these enhancements. TACLAN workstations must provide the capability to identify, integrate, mensurate, and fuse highly accurate positional data, from multiple sources, to provide the requisite tools for worldwide geo-coordinate and datum conversion. SOF intelligence also requires the ability to query, retrieve, and process electro-optical, radar, infrared, multispectral, and video data. Image preparation and exploitation in the processing phase precedes production.

(6). SIGINT. TACLAN workstation must provide the ability to process both current and archival SIGINT products. This includes receipt and processing of real time, near real-time (NRT) and historical SIGINT-derived information in garrison and deployed/tactical environments. This capability must include a SIGINT (i.e. ELINT) correlator capable of depicting threat emitters, with a decision tool capable of depicting lethality zones (threshold). AFSOC systems will have a minimum of ELINT level 2 capability. Other analysis tools include histograms, ops clocks, and audible and message screen notification alarms that are operator selectable (objective). Archival needs include access to current NSA databases (threshold).

(7). OSINT. TACLAN workstations must provide the ability to access, receive, process, and display open source intelligence/information.

(8). Collaboration. Analysts must have a collaboration tool that provides the capability to communicate and share information in a persistent virtual environment, independent of location and time. The collaboration tool should provide advanced collaboration capabilities to facilitate interpersonal communication, data access, and knowledge management. Tools should include electronic whiteboard, audio, chat, shared applications and video, and should be supportive of multiple data and image file formats. The collaboration tool must be platform independent; usable in both a UNIX and Windows environment.

(9). General Military Intelligence (GMI). TACLAN workstations must provide the capability to query, retrieve, display and manipulate general military intelligence databases produced at the national, theater, or tactical levels.

(10). Indications and Warning (I&W). TACLAN workstations must provide the ability to receive, monitor and send critical I&W intelligence in real time.

(11). Language Translation. TACLAN workstations must provide access to Intelligence Community capabilities to translate foreign language documents.

d. Production. The intelligence functional area of production "is the integration, evaluation, analysis and interpretation of information from single and multiple sources into finished intelligence for known or anticipated military and related national security

consumer requirements." (JCS Pub 2-0) SOF intelligence analysts must be capable of providing current in-depth and estimative all-source intelligence products in support of SOF mission requirements. SOF intelligence analysts must be capable of electronically pulling intelligence/ information from multiple sources and media (text, video, imagery, audio) through connectivity with tactical, theater, Service, national and allied/coalition intelligence AIS, and national labs AIS.

(1). Imagery. Imagery production is the preparation of the image transitions into either a raw information or finished intelligence product, such as prints (large and small) or digital transmissions. It includes much of what is required in the processing phase (see paragraph 1.3.5) since there is an inherent overlap between processing and production. Imagery interpretation is conducted in this phase; therefore, an imagery exploitation system should facilitate query, retrieval, annotation and ultimate fusion of multiple image or textual products for analytical/comparative purposes; the inclusion of archival search functions and implied connectivity to worldwide servers/imagery libraries is paramount. The final production of image products should be via peripheral devices, such as printers.

(2). Geospatial Information and Services (GI&S). TACLAN workstations must provide for automated mapping/DTED/orthorectification at numerous, user definable levels of resolution. GI&S applications must be capable of worldwide application on a common datum. SOF intelligence requires the capability to overlay a mensurated grid on acquired soft copy imagery; the capability to query, retrieve, display, and manipulate geospatial databases; and the capability to produce hard copy using large format color printers.

(3). Automated Intelligence Support to SOF Mission Planning. Order of battle and imagery are the two critical intelligence products that automated mission planning systems need to receive from SOF intelligence for effective mission planning. The order of battle updates must come from the fused situation display referenced in paragraph 1.3.1. TACLAN workstations must have the capability to seamlessly (or via electronic media if MLS is not available) export this OB, at the secret level, and in the national standard database schema and formats for general military intelligence. TACLAN workstations must have the capability to export imagery via electronic media in national standard formats for import to automated mission planning systems. As an objective capability, SOF intelligence must be able to provide a seamless electronic feed to mission planning and rehearsal systems. Support to mission planning systems includes the capability to access imagery from national, theater and tactical data bases; generation of 3D perspective views/output (scene visualization / "fly-throughs"); access to threat data, threat libraries, active emitters and emitter historical data; and determination of terrain masking and threat capabilities. NRT broadcasts, and access to joint/Service/theater targeting applications are critical to mission/target planning and execution.

e. Dissemination. The intelligence functional area of dissemination "is the conveyance of intelligence to users in a suitable form." (JCS Pub 2-0) SOF intelligence

analysts are required to publish and disseminate tailored multimedia intelligence products using "push/pull" and exportable mass storage technologies. The requirement is to "publish once and disseminate many times". TACLAN workstations must be able to disseminate products throughout SOF, to include operational elements, and other customers, at all levels of security including SCI, collateral and releasable to combined/coalition forces.

(1). Electronic Publishing. The TACLAN workstation electronic publishing and dissemination capability must provide a seamless interface with theater automated intelligence systems and imagery dissemination systems. This capability must include the ability to move intelligence products seamlessly from the production to the dissemination environment. Dissemination of intelligence products should optimize the use of web-based technology.

(2). Designated SOF producers require the capability to populate intelligence product servers (i.e. INTELINK/INTELINK-S, Image Product Libraries (IPL), Intelligence Data Handling Systems (IDHS)).

(3). Imagery Dissemination. SOF at all operational levels require the capability to access archived soft copy imagery and intelligence products residing on national, theater, service and SOF servers/archives. SOF imagery producers require the capability to populate imagery product servers. Expeditious dissemination of both raw imagery and finished image products is paramount. Connectivity to worldwide image servers and image product libraries is equally necessary. Final dissemination of image products should be accomplished via existing robust communications channels and/or courier means. The SOF imagery architecture should support the unimpeded 2-way transfer of softcopy and hardcopy imagery from/to tactical, operational, and strategic echelons of SOF command. Dissemination of imagery must include optical medium. Additionally, SOF capability must include the dissemination of tactical imagery from sources such as digital cameras.

(4). Hardcopy Dissemination. Require high speed, photo quality print capability to provide hard copy imagery and other intelligence products at the SOF mission planning level.

(5). Health Services Dissemination. TACLAN FCD capability must include the ability to move SOF HS seamlessly from the point-of-exposure/care to the dissemination environment.

(6). VTC Dissemination. As an objective capability, TACLAN workstations require the ability to utilize video-teleconferencing (VTC) as a means of dissemination.

(7). NRT Broadcast Dissemination. As an objective capability, TACLAN workstations must be able to inject and receive products for dissemination via NRT broadcast dissemination systems (e.g. GBS).

10. Electromagnetic Environmental Effects (E3) and Spectrum Supportability.

a. Electromagnetic Environment. During crisis or conflicts, U.S. communications are threatened by physical destruction, capture, and the full spectrum of offensive information operations that include network attacks, exploitation, and electronic warfare. General warfare adds attacks from direct and indirect fire, NBC munitions, electromagnetic pulse (EMP), and directed energy weapons. Equally as important as the Electromagnetic Environment impacts is the impact adverse space weather events can have on RF, HF, VHF, UHF, and/or SATCOM communications. The development of new communications capability should account for and seek to mitigate as best possible within the current state-of-the-science negative impacts from adverse space weather events.

b. Electromagnetic Compatibility (EMC). TACLAN solutions shall be EMC within itself and with other systems in its operating environment, such that system operational performance requirements are met. System performance requirements shall be met while operating in the electromagnetic environment produced by weapon detonation, RF weapons and/or other IW devices. The TACLAN solutions, and all subsystems supporting those solutions EMC (including COTS and NDI), shall comply with the applicable DOD, National, and International E3 and spectrum management policies and regulations.

c. Radio Frequency Spectrum Supportability. Procurement or acquisition of all wireless radio frequency (RF) dependent devices, to include commercial off the shelf (COTS) and non-developmental items (NDI), must be conducted IAW DoD and MILDEP policy/directives (i.e. DoDD 4650.1). TACLAN employs a spiral development, technology insertion, or block upgrades and must obtain equipment allocation guidance/status during the planning stages. PMs normally obtain equipment allocation guidance by submitting a DD Form 1494, "Application for Equipment Frequency Allocation" through their supporting spectrum management office. PMs must ensure RF support in the countries determined by the PM or procurer for the equipment's intended use. If the equipment is to be used outside US&P, a DD Form 1494 must be generated as releasable to the countries of interest and must be sent through spectrum management channels to the theater Combatant Command commander, who will coordinate and obtain host nation equipment allocation and spectrum supportability comments. Once the equipment allocation process is complete, the user can request specific operating frequencies through the appropriate spectrum management office.

11. Assets Required to Achieve Full Operational Capability (FOC). FOC will occur when 100% of all equipment and upgrades is fielded to units. However, because TACLAN is fiscally constrained FOC will probably not occur. Additionally, because of the program's evolutionary acquisition strategy and continuing upgrades FOC will not occur.

12. Schedule and Initial Operational Capability (IOC)/FOC Definitions. The primary objective of the TACLAN Acquisition Strategy is to minimize both the time and costs of program development, consistent with common sense and sound business practices.

TACLAN will be developed using an incremental "build-test-build" approach. A TACLAN LRIP has been developed for the purpose of demonstration and evaluation. This "event driven" development will link program decisions to demonstrated accomplishments in development, testing initial production leading to Initial Operating Capability within a significantly shortened development cycle. Fielding will not take place until a successful Production Qualification Testing (PQT) / Initial Operational Testing (IOT), F&DR, and security accreditations are conducted/obtained.

a. Initial Operational Capability (IOC). IOC will be declared when one network suite of equipment configurable from one to all three networks operating at any of the three classification levels (i.e., Unclassified, SECRET, TS-SCI) is fielded to each of the Theater Special Operations Commands (TSOCs), and each of the Components. Planned for August 2004.

b. Full Operational Capability (FOC). In addition to being fiscally constrained, FOC will most likely not occur because of the program's evolutionary acquisition strategy.

13. Other Doctrine, Organization, Training, Material, Leadership and education, Personnel, and Facilities (DOTMLPF) Considerations.

a. General. TACLAN will consist primarily of equipment and parts from COTS/GOTS resources which are compliant with industry and DOD standards and open systems architecture in order to minimize problems with interoperability and standardization and to reduce costs associated with specialized military equipment. TACLAN will not provide power generation units and/or other base operating support (tents and environmental control units (ECUs)). No new unique firmware will be developed requiring computer resources support. The USSOCOM Common Information Technology Base Line (CIBL) will be used to identify components that can be used as a part of TACLAN. This will involve the identification and distribution of hardware and software standards, commercial software modifications, database maintenance, and introduction of new software packages. Users will identify hardware and software requirements, which will be validated through a formal configuration control board process. The USSOCOM Chief Information Officer (CIO) is responsible for maintaining the USSOCOM CIBL.

b. Logistics and Readiness. The TACLAN (consisting primarily of equipment and parts from COTS/GOTS resources) maintenance plan must ensure that frequency and duration of preventive and corrective maintenance activities will have minimal impact on users and will comply with system performance parameters listed above and vendor maintenance schedules. In addition, the maintenance plan must accommodate sufficient spares for approved mission critical network components.

c. Maintenance Planning. TACLAN equipment will have an initial manufacturer's warranty of 3 years. Extended warranties will be considered. Contractor warranty service will be used when cost effective. The TACLAN maintenance concept is comprised of two levels of maintenance: organizational and above organizational

maintenance. Organizational level (O level) maintenance is the equivalent to unit level maintenance and will include unit personnel performing preventive maintenance, checks and services (PMCS), removal and replacement of major end-items or components, cable replacement, and minor hardware replacement (network cards, hard/floppy/CD-ROM drives, fuses, batteries, etc.). Anything requiring maintenance beyond simple "remove and replace" will be returned to an above O level maintenance capability. This could be accomplished by the Original Equipment Manufacturer (OEM) or an organic/contract source of repair. Above O level maintenance entails all maintenance beyond the established capabilities of the O level including direct support, general support, and depot-level maintenance. Where feasible, there will be plans for on-site contractor support to be available when the system is deployed. Maintenance technicians may be required to wear chemical warfare gear while performing periodic maintenance or repair. No special tools will be required to do routine maintenance. Decontamination procedures will be addressed in appropriate technical manuals. A help desk function at a central point is also desired. The TACLAN will include a diagnostic capability that will automatically notify system administration personnel by email, or other automated means, of system failures and malfunctions. The system will automatically generate a log for system usage and errors.

d. Maintenance Management. The organizational deployed network system administrators/technicians will monitor and manage the TACLAN system, and provide assistance to users with questions about software and hardware. They will assist in coordinating contractor repairs or equipment replacement. They will file maintenance request and schedule maintenance personnel to assist users. They are responsible for maintaining preventive and corrective maintenance records, and compiling a maintenance history for the TACLAN system. The history will be used to forecast maintenance requirements, schedule maintenance resources, and develop a comprehensive spares policy.

e. Deployed/field level maintenance. Deployed/field level maintenance will be in a tactical environment where commercial power and environmentally controlled conditions may not exist. The deployed location will maintain a 24 x 7 control point for reporting and coordinating repair and replacement efforts. Operational constraints will limit the amount of personnel, test equipment, tools, and available spares at a deployed location. Operators will swap out major end items such as workstations, monitors, switches, routers, and hubs. Periodic maintenance will be accomplished at the deployed/field level. Maintenance functions will be performed primarily through internal systems diagnostics/self tests. System diagnostic logs will be automatically generated so field personnel can send to base/home units for recording/trend analysis purposes. Field repair of components will be allowed without voiding warranty.

f. Support Equipment. TACLAN will require standard network management diagnostics software tools, but no special test, maintenance, measurement or diagnostic equipment. No unique or peculiar support equipment is desired. If specialized support equipment is required, it will be provided with the equipment.

Support equipment must fit the same packaging/transportation specifications as the supported equipment.

g. C4I/Standardization, Interoperability, and Commonality.

(1). Standardization Requirements. TACLAN must comply with the following standards:
Current versions of DII/COE interface specifications (Level 6) and DOD JTA version, 3.1 31 March 2000. User Interface Specifications for DII, Joint Interoperability and Engineering Organization, Defense Information Systems Agency, Washington DC, 1 April 1996. Future standardization requirements will be in accordance with Net-Centric Enterprise Services (NCES) documentation.

(2). Interoperability Requirements. TACLAN must provide seamless interoperability that allows for information transfer and assurance into the GIG. Information systems that perform the same function must be common, unless specific mission analysis determines they should be unique. Open systems architecture will be achieved by the use of JTA standard interfaces, formats, and protocols to facilitate interoperability in a multi-vendor, heterogeneous environment. . As it is modernized it will continue to interoperate and progress along the same communications-electronics modernization paths as the rest of the DOD. It must effectively receive, process, and transmit all applicable operations and data protocols, as well as applicable intelligence information. The system will incorporate an open C4I architecture that will enable it to receive all data inputs to provide the best battlespace picture. The C4I architecture will also enable TACLAN to communicate necessary operations, data, and imagery information to other C4ISR elements. As TACLAN migrates into the networking environment to pass critical information the need for Information Assurance is greatly increased. Information products required for sharing with other C4ISR facilities will be labeled utilizing standardized metadata and retains its form. All IDM applications (COTS or GOTS) will adhere to DOD Chief Information Officer (CIO) prescribed National Security System (NSS) and Information Technology System (ITS) standards and comply with all IDM requirements within the GIG CRD. The System Program Manager shall develop a Command, Control, Communications, Computers, and Intelligence Support Plan (C4ISP) IAW the DOD Regulation 5000.2-R to address C4I interoperability and supportability requirements/deficiencies. Transport systems shall maintain and guarantee the integrity of all information elements exchanged throughout the GIG to enable user confidence; information integrity shall be 99.99% (THRESHOLD) and 99.999% (OBJECTIVE).

(3). Commonality Requirements (Common Baseline). In coordination with the TSOCs and Components, the TACLAN Program shall establish a common baseline for the acquisition of C4I related hardware and software. Computer network related items will be selected so that they fit the requirements of USSOCOM C4IAS affiliated systems. The purpose of this requirement is to eliminate the use of a wide range of hardware and software to satisfy a common requirement. This will lessen the logistics requirements associated with the lifecycle support of the USSOCOM C4I infrastructure.

Intelligence functions will be incorporated as per the current SOCRATES baseline and will be functionally interoperable with all current and future intelligence systems. Intelligence functions are listed in appendix F.

h. Geospatial Information and Services (GI&S). TACLAN workstations must provide for automated access and capability to annotate/manipulate geospatial products. High-resolution digital terrain elevation data (DTED) at all levels is critical to SOF mission planning and rehearsal capabilities. TACLAN workstations must provide access to maps and charts now available on CD ROM/soft copy in vector format, with the capability to print to a color printer. Intelligence analysts also require automated tools to support topographic, hydrographic, oceanographic, and weather analysis.

i. Computer Resources. Computer resources will use COTs workstations and accommodate the fundamental concepts associated with TACLAN program: the use of evolutionary system enhancements, rapid prototyping, extensive user involvement, integration of COTS/GOTS components, and integration of existing and new software packages. The system hardware must be modular and facilitate growth. TACLAN setup and system initiation shall be simplified and not take longer than the setup and initialization of the remaining LAN operational environment. Administration will be accomplished organically. TACLAN workstations and servers shall employ a standard GUI to launch applications or to display information in response to operations, maintenance, or other selection categories using a menu- and/or icon-based service.

j. Other Logistics and Facilities Considerations.

(1). Supply Support. Provisioning strategy will be established by the logistics support activity. Spare parts must be available for the life expectancy of the equipment. If equipment is COTS, spare management will be provided in accordance with vendor support concepts. Sparing will be to the equipment level, with little need to open equipment to replace components, unless it is the standard commercial practice. Procedures for obtaining and tracking parts must be identified at time of equipment selection. Readiness Spares Packages (RSP) will be developed to support deployments with the ability to tailor the package to mission needs and requirements. RSP equipment must be kept up to date with the current equipment TACLAN is using. RSPs will be kept in a centralized location as determined by the logistics support manager until the equipment is requested to support a forward location. Logistics Manager, USSOCOM CIO representative and the component representative will determine optimal forward based location based on current situation.

(2). Facilities. Equipment will not require any specialized operation or maintenance facilities. There are no unique shelter requirements. TACLAN will be operated in environmentally controlled tents or buildings. Although TACLAN will be operated in a sheltered environment, it may be exposed for prolonged periods to outside environments while in transport or while stored in tactical areas.

(3). Packaging, Handling, Storage, and Transportation. TACLAN does not present any unusual transportability, packaging or handling requirements. Each TACLAN transit case must facilitate two-person carry. The TACLAN must be transportable in its transit cases as restrained cargo in vehicles over primary roads, secondary roads, and cross-country and by air, ship, and rail. System will fit on standard aircraft pallets. TACLAN assets will require no special storage facilities. Estimated storage space for a TACLAN system is 912 cubic feet.

(4). Manpower and Personnel. No additional military manpower will be made available to support TACLAN. Personnel will be required to perform systems administration functions in support of the TACLAN. The manpower necessary to operate, maintain, support, and train TACLAN will be within the SOF Component force structure. Full operational deployment of TACLAN will not increase the SOF Component end strength. No new occupational specialties will be required to operate or maintain TACLAN equipment. System may require modification of existing specialties.

(5) Force Structure. TACLAN will support organizations from the TSOC down to the team/element level. The total number of TACLAN systems required will consist of the sum of SOF unit requirements plus maintenance spares, and one system to be used as a test bed assigned to the TACLAN Program Office. TACLAN Basis of Issue (BOIP) Tables are at Appendix E.

(6). Training Concept. The training concept for TACLAN addresses new equipment training, institutional training, and unit sustainment training. Training for TACLAN will leverage existing C4IAS and other garrison training programs. New training for TACLAN will focus only on the unique aspects of deploying and operating the TACLAN system. Mission application program offices will provide the respective mission application training.

(7). Training. The TACLAN program will provide for two forms of system training: Initial System Training and Follow-On System Training. Initial System Training must be provided with the new TACLAN equipment. On-site new equipment training teams will perform unit training during initial equipment fielding. Training packages accompanying the equipment will be included for Systems Administration (to include System Administrator Level I, II, or III certification as needed) and technical personnel. The TACLAN program will provide training via existing government sources, contractor services, or vendor support. Training will be in the form of classroom training supported by self-study CD-ROMs and manuals. Trainers within the respective commands will train those who will be maintaining and supporting TACLAN (Train-the-Trainer). Contract training support will remain available for the duration of any contracts to provide required support and advise commands of updates/changes to software/hardware. Follow-On System Training may use mobile training teams (government, contractor, or vendor) to be deployed on an as needed basis. The unit will have the sole responsibility for sustainment of operator and maintainer proficiency.

(8). COMSEC Training. Instructions for communications security (COMSEC) equipment maintenance and training will be provided using applicable COMSEC materials and guidelines. Equipment with embedded COMSEC will allow maintenance personnel to perform maintenance without compromising security.

14. Other System Attributes.

a. Technical Data Requirements. Commercial level technical data is acceptable and integrated systems level documentation is required, to include set up of workstations. Integrated Logistics Support (ILS) is necessary to assure the effective and economical support of the system. A Supportability Analysis will identify maintenance concepts and characteristics, tools, test equipment, and personnel required for equipment maintenance.

b. Environmental. TACLAN must deploy and operate in field environments where SOF forces deploy. Wind, rain, snow, ice, sand, and dust must be considered for each environmental condition. With the exception of the tactical teams (using FCDs vice TACLAN workstations), TACLAN will be deployed to some kind of sheltered facility (tent, warehouse, building, etc.) with varying degrees of environmental control. The TACLAN workstations and network components will meet the following conditions:

Storage and Transit: -50° F to +160° F (Threshold)
External Operating Temperatures: -50° F to +130° (Threshold) *
Internal Operating Temperatures: +40° F to +90° (Threshold) -20° F to +130° F (Objective)**

* External Operating Temperatures are defined as temperatures outside of the sheltered facility.
** Internal Operating Temperatures are defined as temperatures inside a sheltered facility.
Component equipment temperatures may vary inside of the transit case while in operation as long as they do not exceed the manufacturer's maximum temperature range.

The FCD components must endure outdoor operations in the following conditions to support deployed tactical teams:

Storage and Transit: -50°F to +160° F (Threshold)
Operating Temperatures: 40° F to +120° F (Threshold)

c. HERO. There are no known safety issues regarding hazards of electromagnetic radiation to ordinance.

d. Communications Security Management. All COMSEC levels will be handled IAW National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4001 and other appropriate guidance.

e. NBC Contamination/Survivability. TACLAN equipment will be designed to enable operators to perform equipment tasks (steady state) with degradation (time) while in Mission Oriented Protective Posture IV (MOPP IV) suits and to perform mission tasks to include setup/tear down in an operational environment allowing for degradation (time) considering (internal heat) stress conditions. Terminal devices and non-sheltered components that are contaminated or rendered inoperable due to contamination will be removed for repair determination/discarded or decontaminated according to all applicable practices/procedures.

f. Network Protection and Security. TACLAN will be type accredited, based on network security requirements per DOD Manual 8510.1-M, Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual and Chairman Joint Chiefs of Staff Instruction (CJCSI) 6211.02A, Defense Information System Network and Connected Systems. Standardized network control functions will prohibit unauthorized access to restricted network(s)/information, support continual security and system monitoring capabilities, determine database permissions, and will provide for user log-on anywhere within their network segment (Threshold). TACLAN will use approved security solutions to provide the system administrators with automated capabilities to monitor network activities such as intrusion attempts, audit trails, and system backup status and have the capability to affect defensive electronic responses (e.g., block IP address, disconnect attacker, notify system administrator, trace attack, etc.) (Threshold). TACLAN will use password protection software that shall require unique user identification and password per security level for log-on (Threshold). TACLAN will provide for network recovery from denial of service attacks and will incorporate an automated means for malicious code detection (computer virus) including an update capability at the user and server level (Threshold). TACLAN will provide software to facilitate system backup and restoration. TACLAN will use a functional interface with security elements of higher-level network management systems (Information Dissemination Management, Joint Network Management System (JNMS)) when available, while avoiding duplication of status reporting/services (Objective). TACLAN will use Public Key Infrastructure (PKI) when available (Objective). PKI will consider communications interoperability with commercial and multinational partners during implementation (Objective). Systems shall meet and maintain minimum IA Defense in Depth standards, including certification and accreditation IAW the DITSCAP process (e.g., CJCSI 6510.01C, DODI 5200.40) (Threshold, KPP). TACLAN will integrate with Information Assurance tools as they are developed to include voice/digital signatures, imprint identification, identification and validation of secure protocols, and improved system/network boundary guards (Objective). Content Based Encryption – When available system shall have an IA capability to perform content-based encryption of information objects at the host instead of depending on the bulk encryption of the entire network in order to secure the information (Threshold), and this capability shall also be available for operations involving allied and coalition forces (Objective).

g. Human Factors Engineering.

(1). Design. The system design, to include controls, displays, configuration, connections, required procedures, and operating environment will minimize human performance errors, interface problems, and workload requirements. Human Computer Interface (HCI) must be as uncomplicated and intuitive as possible and must include concerted attention to such characteristics as screen content and layout, menus, help availability, feedback and safeguards, and both ready accessibility and procedural requirements associated with critical tasks/functions.

(2) Ease of Operation. All design and operation aspects of the components/network operating environment must conform to applicable human engineering design criteria to support ease of operation.

h. System Safety/Health Hazard Assessment. The system will be designed in accordance with all applicable system safety standards so as to minimize safety risks associated with operating, maintaining, managing or supporting the system. Any residual hazards or risks associated with installing, operating or maintaining the system or its components must be identified, attended to in training and support materials, and made manageable. Particular emphasis will be placed on minimizing risks of electrical shock and visual strain. A Health Hazard Assessment will be conducted on all new equipment.

i. System Software. TACLAN will use software on the USSOCOM CIBL. TACLAN will provide standard platforms, operating system services and support applications as defined elsewhere in this document. TACLAN is not responsible for the development of mission area applications, nor their test and integration into the TACLAN baseline. The USSOCOM SOF Integration Facility (SIF) will support test and integration of mission area applications into C4IAS and TACLAN and will support the release of the mission application into C4IAS and TACLAN approved software baselines.

15. Program Affordability.

a. General. TACLAN will leverage Service efforts to provide automation support wherever possible, and use MFP-11 funding to fill in gaps in Service provided programs. To further facilitate commonality with Service provided systems, fielding will focus on putting like-systems in the deployed units' hands to prevent the need to support numerous types of hardware/software to perform the same operational functions. TACLAN associated systems migration objectives are tied to evolutionary acquisition practices that are DII/COE compliant and include advanced technology insertions. The implementation of TACLAN's state-of-the-art hardware and communications interface technology will provide the SOF user community with the best, most efficient means to effectively satisfy future SOF information exchange and planning needs.

b. Cost. During the FY02-07 POM, USSOCOM Assessment Directors recognized the need for TACLAN while approving a transition of FY02 funding from existing

affiliated programs to a TACLAN Program funding line. As a result, TACLAN's initial priority should focus on continuing the current level of effort of those affiliated programs (e.g., SOFTACS, JBS, SOCRATES-D, POBS, SOF-IV (M), SOTVS, SOFPARS, et al). Subsequent efforts will formalize the existing decentralized, "end of year" acquisition approach of acquiring deployed networks through a more systematic, standardized acquisition process. In today's fiscally constrained environment, the total system cost may drive limited deployment of the system. Specific fielding prioritization will be decided via the same executive review panels that determine C4IAS fielding distributions. Although FOC will not occur, every effort should be made to keep the acquisition program within budget. Life Cycle Cost (LCC) must be a factor in the acquisition phase and increases in TACLAN LCC must be held to a minimum.. The current estimated costs for TACLAN are outlined in the TACLAN LCC Estimate, (LCCE), dated 14 June 2002, and the details are not included as part of this CDD, for detailed information reference the TACLAN SAMP. The cost parameters including procurement hardware, procurement labor, software, Engineering Change Requests (ECRs), training, and spares. These will be used to evaluate cost equanimity of future production and technology insertion proposals. Hardware costs vary according to the capabilities consistent with system size/quantity and system capability (i.e., Multi-Level Security (MLS), scalability, modularity, and interoperability).

16. Secondary Distribution. Further dissemination of this document is restricted to "Distribution Statement C," U.S. Agencies and their contractors. Request for copies of this document will be referred to USSOCOM SOOP-RV.

APPENDIX A

CRD/CPD CrossWalk

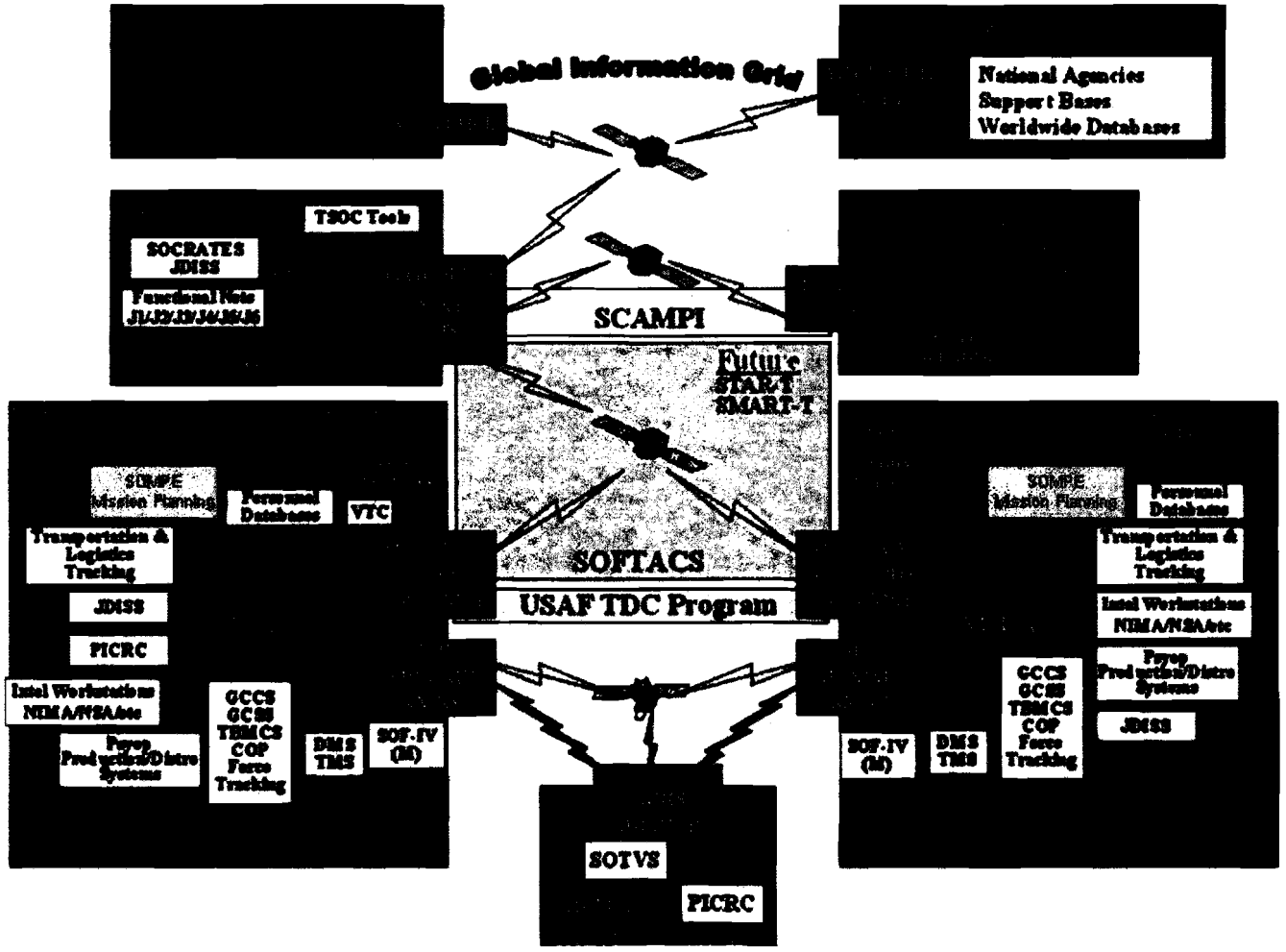
CRD/ICD/CPD	KPP	CPD Page #	CPD Para #	Line #
SIE	Information Assurance		14 f	
SIE	Interoperability		6 c	
SIE	Technology Insertion Capability		6 j	
SIE	Training		13 i (6) (7) (8)	
SIE	Planning		1 b, 3,Table B-1	
SIE	Analysis		Exec Sum, 3, 13 g (2)	
SIE	Rehearsal and Training		Exec Sum, 3, 13 g (2)	
SIE	Execution		Exec Sum, 3, 13 g (2)	
SIE	Positive Command and Control		Exec Sum, 3, Table B-1	
GIG	Interoperability		6 c	
GIG	Store		6 k, l	
GIG	Transport		6 o, Table 3	
GIG	Network Management		6 m, o, Table 3	
GIG	Information Dissemination Management		6 o, Table 3	
GIG	Information Assurance		14 f	

Table A-1 CRD/CPD Crosswalk

APPENDIX B

Integrated Architecture Products

OV-1 High-Level Operational Concept



OV-2 Operational Node Connectivity Description (Needlines) - Provide SOF to GCC Thread

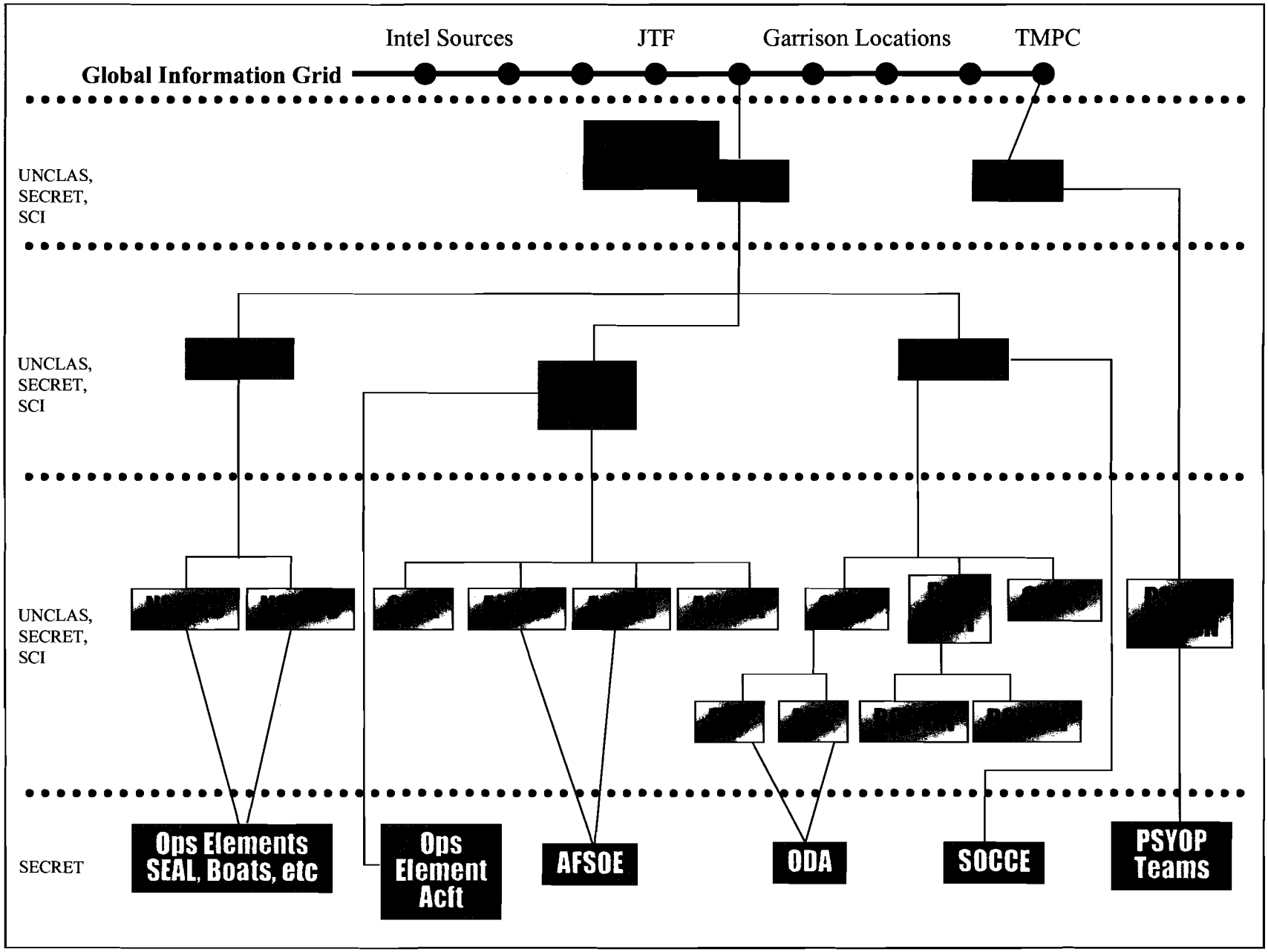


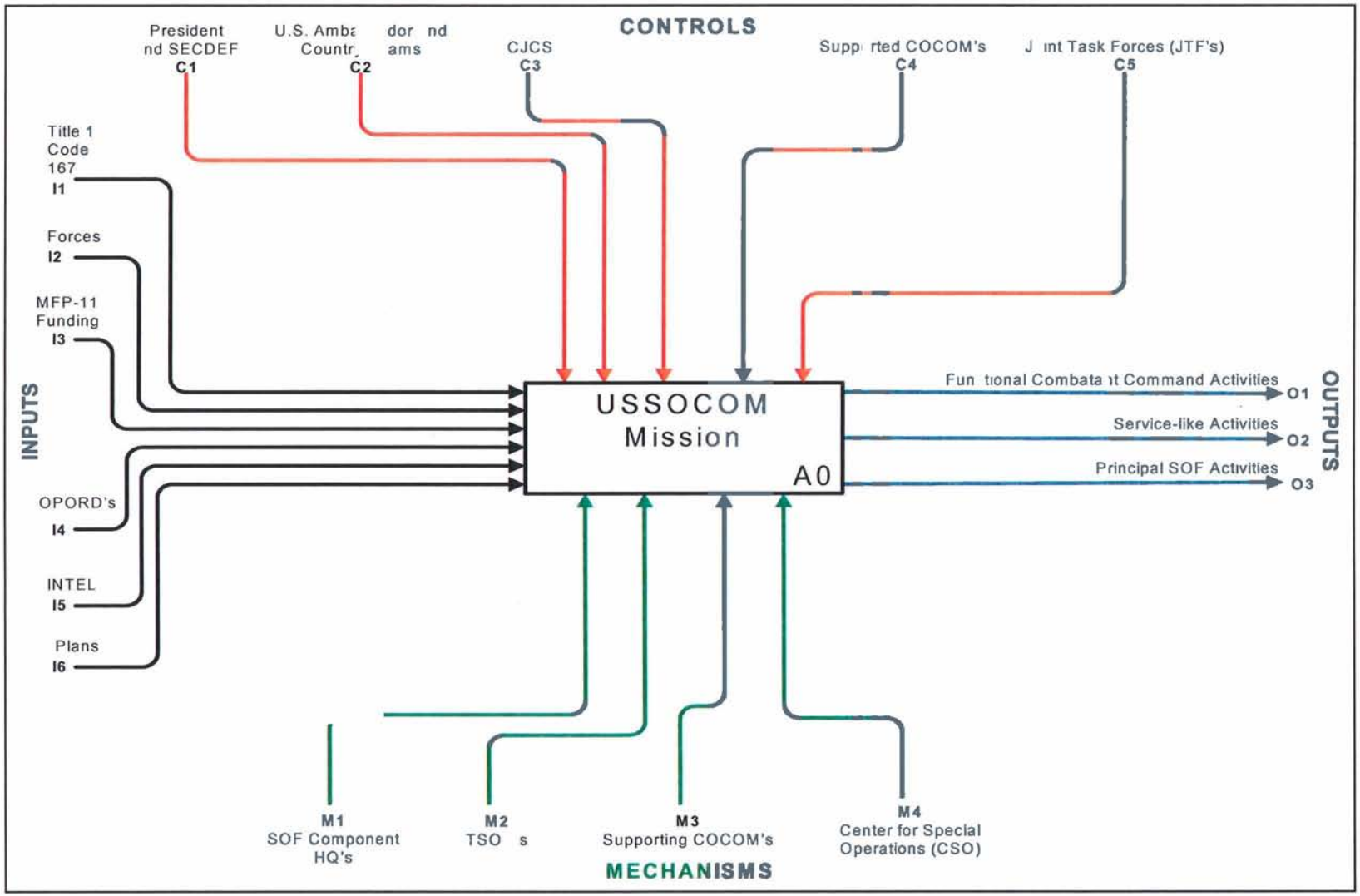
Table B-1. Information Exchange Requirements (IER) OV-3

Rational/ UJTL Number	Event	Information Characterization	Sending Node	Receiving Node	Critical	Format	Timeliness	Class	Remarks
ST 1, ST 3, ST 5, ST 1.1, 5.4,.1,7,.1.3, 8.3.1, 8.3.3 OP 1, OP 3, OP 5, OP 1.1.1, 1.1.3, 1.2.3 5.7.4	Operations planning and reporting	C2--Provide command and control of deployment planning	JSOTF TSOC	SFOB JSOAC NSWTU PSYOP BN CA CMD CA BDE CA BN JTF Higher HQs	Yes	Live Audio Data (< 1 MB) Live Video	NRT 30 Sec NRT	Secret (all formats)	C2 communications to conduct theater strategic operations planning and reporting, full duplex communications
ST 1, ST 5, ST 1.1.3, 8.3.1, 8.3.3, OP 1.1.1, 1.1.3, 1.2.3, 5.5	Force deployment	C2--Conduct intra-theater deployment of forces	JSOTF TSOC	SFOB PSYOP BN CA CMD CA BDE CA BN JSOAC NSWTG	Yes	Live Audio Data (< 1 MB) Live Video	NRT 30 Sec NRT	Secret (all formats)	C2 communications to conduct intratheater deployment, orders dissemination, and force execution, full duplex communications
ST 5, ST 8, ST 1.1, 5.4,.1,7,.1.3, 8.3.1, 8.3.3 OP 5, OP 1.1.1, 1.1.3, 1.2.3 5.7.4, 5.4.2, 5.5	C2 of deployed units	C2—Provide command and control of deploying units	JSOTF	SFOB PSYOP BN CA CMD CA BDE CA BN JSOAC NSWTG	Yes	Live Audio Data (< 1 MB) Live Video	NRT 30 Sec NRT	Secret (all formats)	C2 communications to conduct Theater strategic maneuver and force positioning, full duplex communications
OP 5, TA 1, TA 5, ST 1.1, 5.4,.1,7,.1.3, 8.3.1, 8.3.3 OP 1.1.1, 1.1.3, 1.2.3 5.7.4, 5.4.2, 5.5	C2 of deployed units	C2—Provide command and control of deploying units	SFOB CA CMD JSOAC NSWTU	FOB PSYOP BN CA BDE CA BN NSWTU AFSOD AFSOE	Yes	Live Audio Data (< 1 MB) Live Video	NRT 30 Sec NRT	Secret (all formats)	C2 communications to coordinate control, report readiness, and monitor unit status of significant areas.

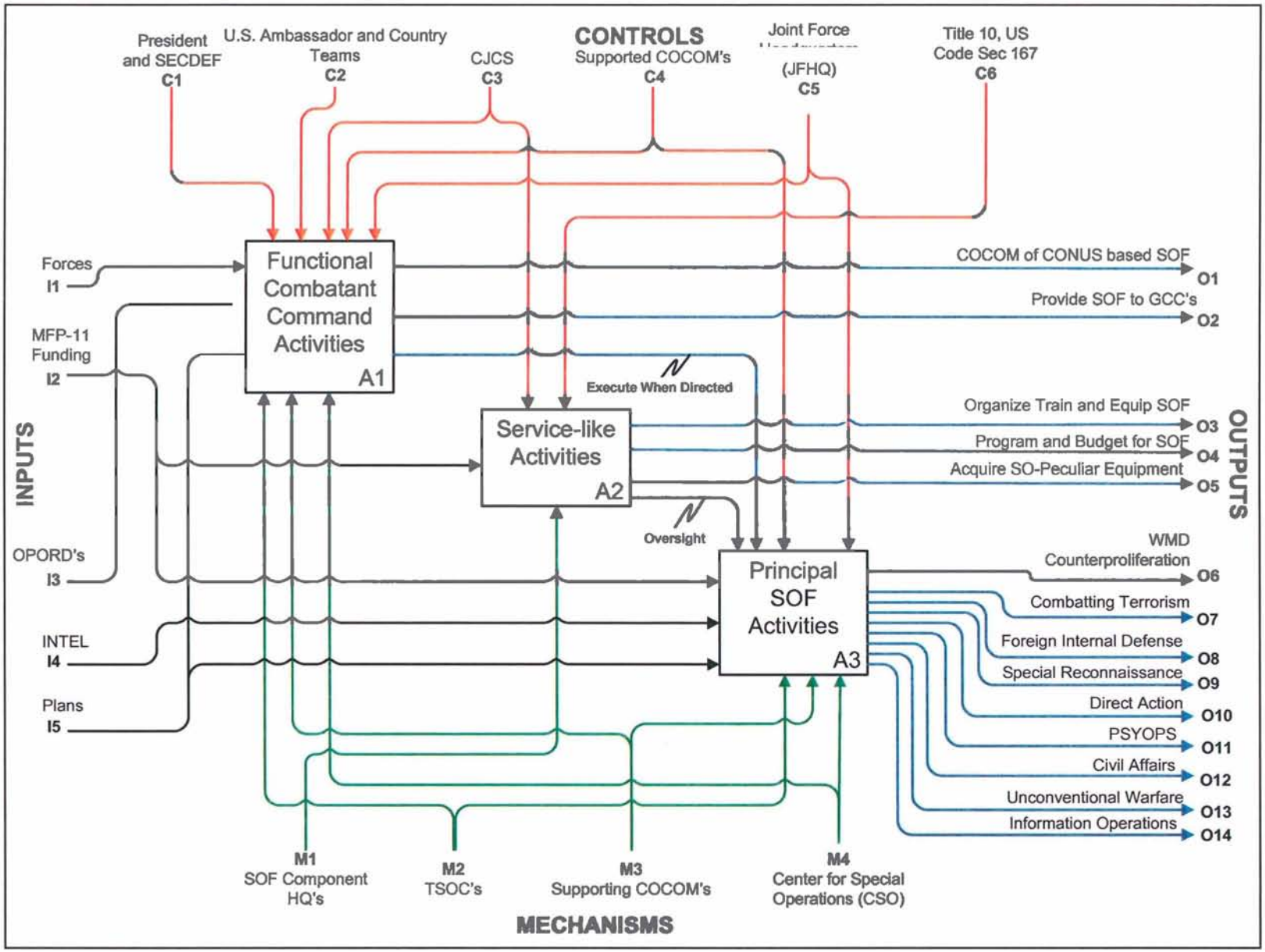
Rational/ UJTL Number	Event	Information Characterization	Sending Node	Receiving Node	Critical	Format	Timeliness	Class	Remarks
OP 5, OP 6, TA 5, TA 6, OP 6.2, 6.2.1, 6.2.5, 6.5, 6.5.3, 6.5.5, ST 6.2.6, TA 6, 6.3,	C2 of C4I	C2--Provide command and control of theater force protection	SFOB CA CMD NSWTG JSOAC	FOB PSYOP BN CA BDE CA BN NSWTU AFSOD AFSOE	Yes	Live Audio Data (< 1 MB)	NRT <30 Sec	Secret (all formats)	C2 communications to conduct theater protection to include security and search and rescue, full duplex communications
ST 2, ST 3, OP 2, OP 3, OP 2.4.1, 2.4.1.1, 2.5, ST 2.1.1, 2.1.3, 2.2.1, 2.3, 2.4.1.2, 8.1.4	Acquire and produce information that supports the intelligence functions	Situation Awareness—Intel collection, threat analysis, target ID, METOC	JSOTF TSOC	SFOB PSYOP BN CA CMD CA BDE CA BN JSOAC NSWTU JTF HHQ	Yes	Live Audio Data (< 10 MB) Live Video	NRT <1 Min NRT	UNCLAS SECRET TS/SCI (all formats)	C2 communications of operational information providing intelligence analysis and reporting to include strategic surveillance, reconnaissance, METOC, and target information
OP 2, OP 3, OP 2.5, 3.1.1, 3.1.3, 3.2.7, ST 2.2.1, 2.4.1.2, 2.4.2.2, 2.2.2.4	Acquire info that supports the detection, ID, and location of enemy targets	Situation Awareness—Intelligence collection, target ID, target location, target track updates	FOB PSYOP BN CA BDE CA BN NSWTU AFSOD AFSOE	SFOB CA CMD NSWTG JSOAC And higher	Yes	Live Audio Data (< 10 MB) Live Video	NRT <1 Min NRT	UNCLAS SECRET TS/SCI (all formats)	C2 communications of operational information providing intelligence analysis and reporting to include strategic surveillance, reconnaissance, METOC, and target information
ST 4, OP 4, TA 4, OP 5.1.4, ST 4.2.2, 5.6.3, 8.2.6,	Operational Logistics, Medical, and Personnel Support	Personnel, Medical, and Logistics--Provide coordination of personnel and logistics support	AFSOC JSOTF SFOB PSYOP BN CA CMD CA BDE CA BN NSWTG FOB NSWTU	AFSOD AFSOE JSOTF SFOB FOB PSYOP BN CA CMD CA BDE CA BN NSWTG NSWTU	No	Live Audio Data (< 1 MB) Live Video	NRT 30 Sec NRT	UNCLAS SECRET (all formats)	Coordination and control of personnel, medical, and logistical support and planning, full duplex communications.

Rational/ UJTL Number	Event	Information Characterization	Sending Node	Receiving Node	Critical	Format	Timeliness	Class	Remarks
OP1, OP 5, TA 1, TA 5, OP 1.2.4.5, 1.2.4.6, 1.2.4.6, 1.2.4.7, 1.2.4.8, 1.2.5, 1.2.6, 1.3.4, 2.2.2, 2.4.1.2, 3.1.5, 3.2.2.1, 3.2.5.3, 3.2.7, 4.7.2, 5.1.3, 5.4.2, 5.4.4, 5.7.4, 6.2.5, 6.2.6, TA 6.2	Operational Command and Control	C2--Command and Control	AFSOC JSOTF SFOB CA CMD NSWTG	AFSOD AFSOE SFOB FOB PSYOP BN CA CMD CA BDE CA BN NSWTU	Yes	Live Audio Data (< 1 MB) Live Video	NRT 30 Sec NRT	Secret (all formats)	C2 planning and operational guidance of deployed forces and communications assets
ST 2, ST 3, ST 5, OP 2, OP 3, OP 5, OP 2.4.1, 3.1.3, 3.2.7, 5.3.1,	Mission Planning and Analysis	Provide for mission planning analysis and data exchange	JSOTF	SFOB PSYOP BN CA CMD CA BDE CA BN JSOAC NSWTU	Yes	Live Audio Data (1 MB) Live Video	NRT 30 Sec NRT	Secret (all formats)	Coordination of mission planning and analysis, full duplex communications
ST 5, OP 5, TA 5, OP 2.4.1, 3.1.3, 3.2.7, 5.3.1,	Mission Rehearsal	Provide mission rehearsal display for deploying units	JSOTF	SFOB CA CMD JSOAC NSWTU	Yes	Live Audio Data (< 5 MB) Live Video (	NRT <1 Min NRT	Secret (all formats)	Conduct mission rehearsal, full duplex communications

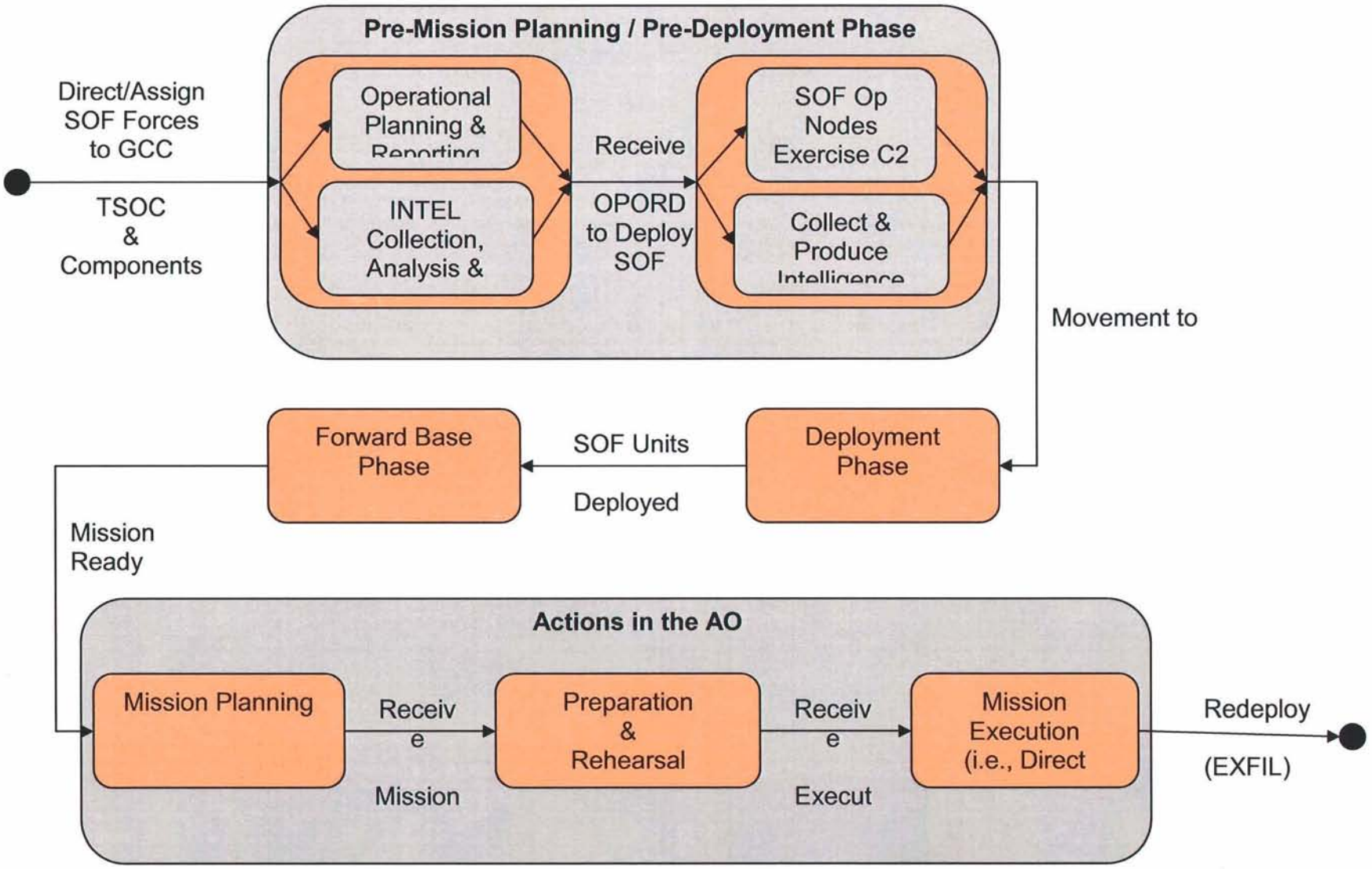
OV-5 Operational Activity Model (pt1)

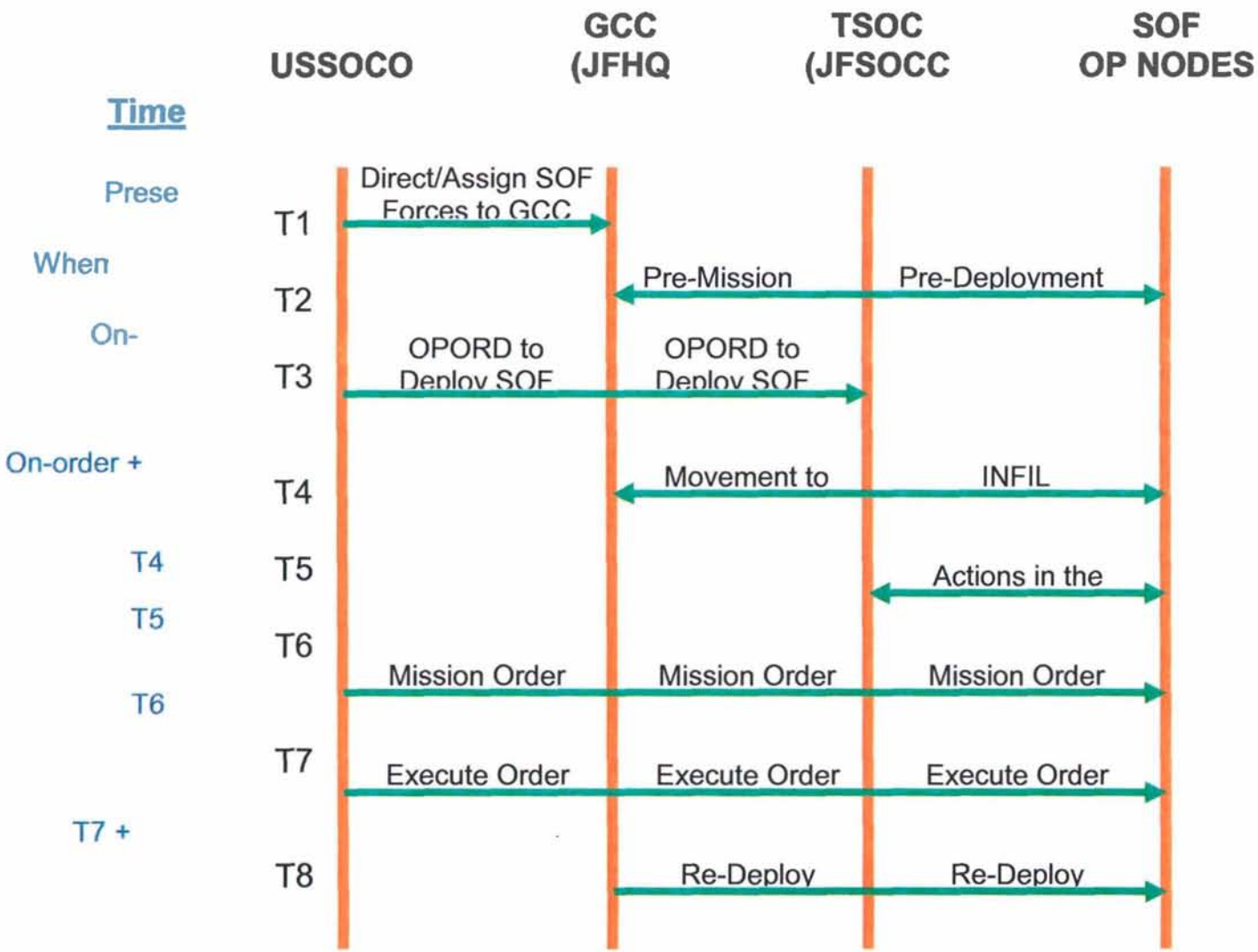


OV-5 Operational Activity Model (pt2)

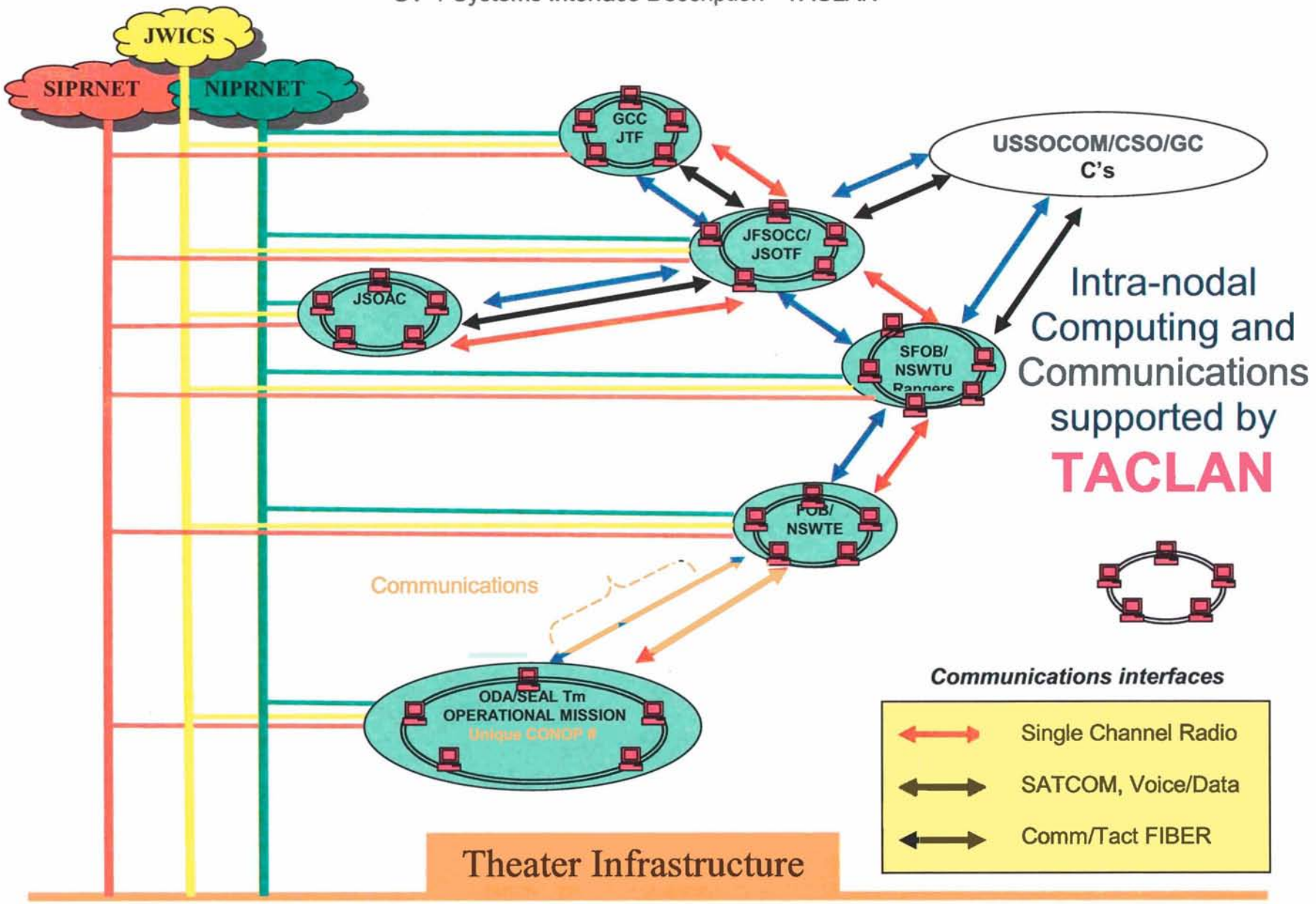


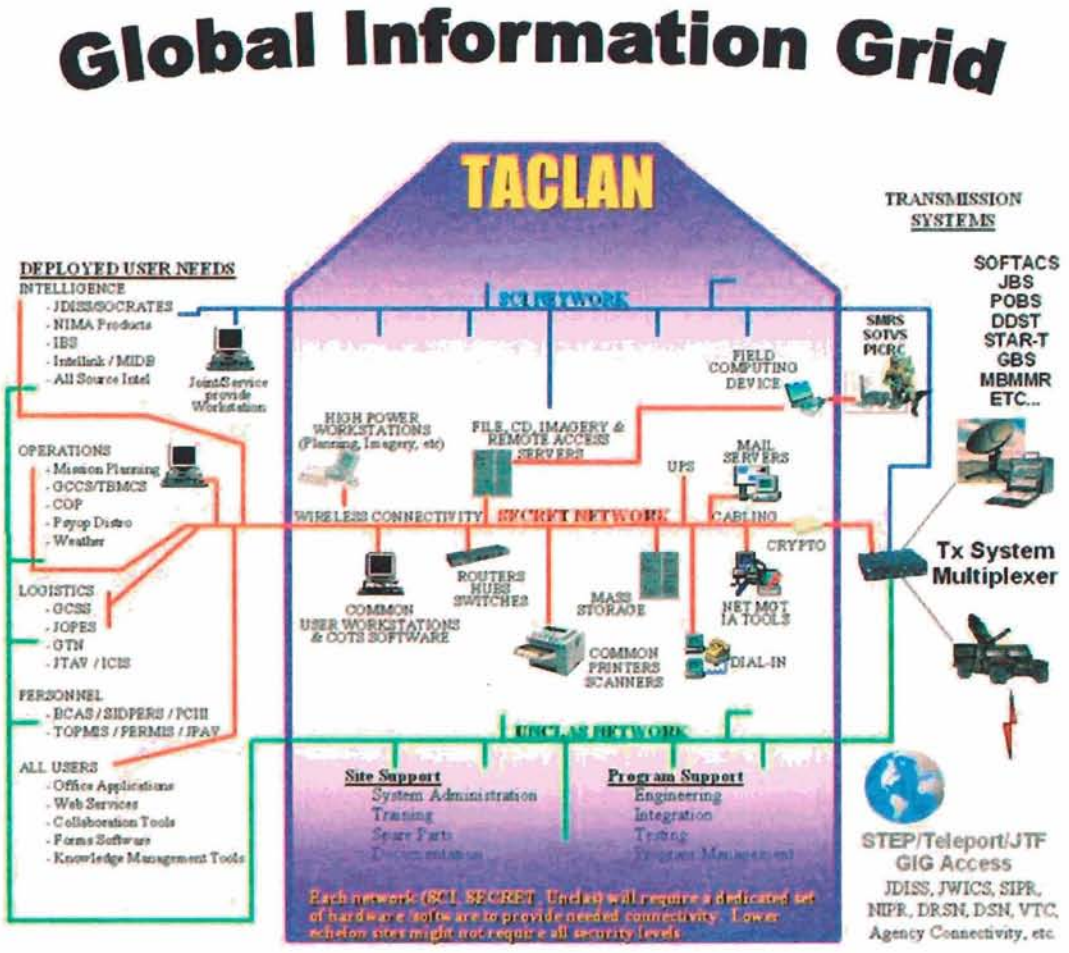
OV-6b Operational State Transition Description - Functional Combatant Command/Principal SOF Activity Thread




USSOCO
GCC (JFHQ
TSOC (JFSOCC
SOF OP NODES
Time
Prese
When
On-
On-order +
T4
T5
T6
T7 +
T1
T2
T3
T4
T5
T6
T7
T8
Direct/Assign SOF Forces to GCC
Pre-Mission
Pre-Deployment
OPORD to Deploy SOF
OPORD to Deploy SOF
Movement to
INFIL
Actions in the
Mission Order
Mission Order
Mission Order
Execute Order
Execute Order
Execute Order
Re-Deploy
Re-Deploy

SV-1 Systems Interface Description - TACLAN




Global Information Grid
TACLAN
TRANSMISSION SYSTEMS
SOFTACS
JBS
POBS
DDST
STAR-T
GBS
MBMMR
ETC...
DEPLOYED USER NEEDS
INTELLIGENCE
- JDISS/SOCRATES
- NIMA Products
- IBS
- Intellink / MIDB
- All Source Intel
Joint Service provide Workstation
OPERATIONS
- Mission Planning
- GCCS/TBMCS
- COP
- Psyop Distro
- Weather
LOGISTICS
- GCSS
- JOPES
- GTN
- JTAV / ICIS
PERSONNEL
- BCAS / SIDPERS / PCIII
- TOPMIS / PERMIS / JPAV
ALL USERS
- Office Applications
- Web Services
- Collaboration Tools
- Forms Software
- Knowledge Management Tools
SECRET NETWORK
HIGH POWER WORKSTATIONS (Planning, Imagery, etc)
FILE, CD, IMAGERY & REMOTE ACCESS SERVERS
FIELD COMPUTING DEVICE
SMRS
SOTVS
PICRC
MAIL SERVERS
UPS
WIRELESS CONNECTIVITY
CABLING
CRYPTO
Tx System Multiplexer
ROUTERS HUBS SWITCHES
MASS STORAGE
NET MGT IA TOOLS
COMMON USER WORKSTATIONS & COTS SOFTWARE
COMMON PRINTERS SCANNERS
DIAL-IN
UNCLASSIFIED NETWORK
Site Support
System Administration
Training
Spare Parts
Program Support
Engineering
Integration
Testing
Each network (SCI, SECRET, Unclass) will require a dedicated set of hardware, softw are to provide needed connectivity. Lower echelon sites might not require all security levels
STEP/Teleport/JTF
GIG Access
JDISS, JWICS, SIPR, NIPR, DRSN, DSN, VTC, Agency Connectivity, etc.

SV-5 Operational Activity to System Function Traceability Matrix
- Functional Combatant Command/Principal SOF Activity Thread

System Functions	**Operational Activities**							
	Functional Combatant Command Activities	Exercise COCOM of CONUS based SOF	Provide SOF To GCC's	Perform Service-like Activities (Title 10)	Organize, Train and Equip SOF	Program & Budget for SOF	Acquire SO-Peculiar Equipment	Execute and Oversee Principal SOF Activities (Missions)
Provide Computers and supporting IT Hardware and Software	X		X	X	X	X	X	X
Provide Automated Mission Planning & Rehearsal	X	X	X		X	X	X	X
Provide Electronic Message Handling	X		X	X	X		X	X
Provide IT Networking Support (Continuity of Operations)	X	X	X	X	X		X	X
Provide Graphics and Mil Std Display of Symbols and Icons	X	X	X		X		X	X
Provide IA and Data and IT Systems Protection	X	X	X	X	X		X	X
Automated Record and Archiving of Systems data	X	X		X	X	X	X	X
Provide for Evolutionary Technology Insertion	X			X	X	X	X	X

SV-6 System Data Exchange Matrix (relative to TACLAN)

Needline	Operational Information Exchange	Performance Requirements	IA Attributes	Threats	Operational Environment
JSOTF/ARSOF	C2, SA, PERS, Med, Log, Mission Planning and Analysis	JTA compliant interoperability KPP	Defined within Security Accreditation Authorization (SAA), to TS/SCI	CA (hacking), Tempest	Sheltered, Deployed
JSOTF/NAVSOF	C2, SA, PERS, Med, Log, Mission Planning and Analysis	JTA compliant interoperability KPP	Defined within Security Accreditation Authorization (SAA), to TS/SCI	CA (hacking), Tempest	Sheltered, Deployed
JSOTF/AFSOF	C2, SA, PERS, Med, Log, Mission Planning and Analysis	JTA compliant interoperability KPP	Defined within Security Accreditation Authorization (SAA), to TS/SCI	CA (hacking), Tempest	Sheltered, Deployed
ARSOF/SFOB	C2, SA, PERS, Med, Log, Mission Planning and Analysis	JTA compliant interoperability KPP	Defined within Security Accreditation Authorization (SAA), to TS/SCI	CA (hacking), Tempest	Sheltered, Deployed
SFOB/FOB	C2, SA, PERS, Med, Log, Mission Planning and Analysis	JTA compliant interoperability KPP	Defined within Security Accreditation Authorization (SAA), to TS/SCI	CA (hacking), Tempest	Sheltered, Deployed
ARSOF/RGR RGT	C2, SA, PERS, Med, Log, Mission Planning and Analysis	JTA compliant interoperability KPP	Defined within Security Accreditation Authorization (SAA), to TS/SCI	CA (hacking), Tempest	Sheltered, Deployed

RGR RGT/RGR BN	C2, SA, PERS, Med, Log, Mission Planning and Analysis	JTA compliant interoperability KPP	Defined within Security Accreditation Authorization (SAA), to TS/SCI	CA (hacking), Tempest	Sheltered, Deployed
ARSOF/CMOC	C2, SA, PERS, Med, Log, Mission Planning and Analysis	JTA compliant interoperability KPP	Defined within Security Accreditation Authorization (SAA), to TS/SCI	CA (hacking), Tempest	Sheltered, Deployed
ARSOF/SOCCE	C2, SA, PERS, Med, Log, Mission Planning and Analysis	JTA compliant interoperability KPP	Defined within Security Accreditation Authorization (SAA), to TS/SCI	CA (hacking), Tempest	Sheltered, Deployed
NAVSOF/NSWTU	C2, SA, PERS, Med, Log, Mission Planning and Analysis	JTA compliant interoperability KPP	Defined within Security Accreditation Authorization (SAA), to TS/SCI	CA (hacking), Tempest	Sheltered, Deployed
NSWTU/SEAL ELEM	C2, SA, PERS, Med, Log, Mission Planning and Analysis	JTA compliant interoperability KPP	Defined within Security Accreditation Authorization (SAA), to TS/SCI	CA (hacking), Tempest	Sheltered, Deployed
AFSOF/JSOLE	C2, SA, PERS, Med, Log, Mission Planning and Analysis	JTA compliant interoperability KPP	Defined within Security Accreditation Authorization (SAA), to TS/SCI	CA (hacking), Tempest	Sheltered, Deployed
AFSOF/AFSOD	C2, SA, PERS, Med, Log, Mission Planning and Analysis	JTA compliant interoperability KPP	Defined within Security Accreditation Authorization (SAA), to TS/SCI	CA (hacking), Tempest	Sheltered, Deployed

AFSOF/ARSOA	C2, SA, PERS, Med, Log, Mission Planning and Analysis	JTA compliant interoperability KPP	Defined within Security Accreditation Authorization (SAA), to TS/SCI	CA (hacking), Tempest	Sheltered, Deployed
AFSOF/Ops A/C	C2, SA, PERS, Med, Log, Mission Planning and Analysis	JTA compliant interoperability KPP	Defined within Security Accreditation Authorization (SAA), to TS/SCI	CA (hacking), Tempest	Sheltered, Deployed
AFSOD/AFSOE	C2, SA, PERS, Med, Log, Mission Planning and Analysis	JTA compliant interoperability KPP	Defined within Security Accreditation Authorization (SAA), to TS/SCI	CA (hacking), Tempest	Sheltered, Deployed

- Joint Technical Architecture (JTA)
- TACLAN Key Performance Parameter's
- TACLAN Requirements Correlation Matrix

APPENDIX C

References

a. DOD Memorandum, 23 October 2000, "Mandatory Procedures MDAPs and MAIS Acquisition Programs."
b. Title 10, United States Code, sections 151, 153, 154, 155, 161, 162, 163, 166, 167, 181, 2223, 3013, 5013, and 8013.
c. CJCS Instruction 3010.02A, 15 Apr 2001, "Joint Vision Implementation Master Plan (JIMP)"
d. CJCS Instruction 3137.01B, 15 Apr 2002, "The Joint Warfighting Capabilities Assessment Process."
e. CJCS Instruction 3170.01C, 24 June 2003, Requirements Generation System
f. CJCS Instruction 3451.01, 1 April 1999, "CINC Field Assessment."
g. CJCS Instruction 5123.01A, 8 Mar 2001, "Charter of the Joint Requirements Oversight Council."
h. CJCS Instruction 6212.01B, 8 May 2000, "Interoperability and Supportability of National Security Systems and Information Technology Systems."
i. CJCS Instruction 6510.01C, 1 May 2001, "Defensive Information Operations Implementation."
j. CJCS Instruction 6721.01, 27 Nov 2000, "Global Command and Control Management Structure."
k. CJCS Manual 3170.01 27 Jun 2003, Operation of the Joint Capabilities Integration and Development System.
l. DOD Directive 8000.1, 27 Feb 2002, "Defense Information Management (IM) Program."
m. DOD Directive 4630.5, 1 November 2002, " Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems."
n. DOD Directive 5100.1, 1 Aug 2002, "Functions of the Department of Defense, and it's Major Components, "
o. DOD Directive 5100.3, 15 Nov 1999 Change 1 23 Mar 2000, "Support of the Headquarters of Unified, specified, and Subordinate Joint Commands".
p. DOD Joint Technical Architecture Version 4, 17 Jul 2002
q. JROCM 032-97, 31 March 1997, "JROC Administrative Guide."
r. C4ISR Architecture Framework, Version 2.0, 18 December 1997.
s. Public law 105-261, Strom Thurmond National Defense Authorization Act for FY 1999, Sec. 331.
t. DOD 5200.1-PH, April 97 "DOD Guide to Marking Classified Documents.
u. USJFCOM GIG CRD, 30 August 2001, JROCM 134-01.
v. USSOCOM C4IAS ORD, 2 January 2002
w. USSOCOM SIE CRD, 14 September 2000

APPENDIX D ACRONYM LIST

AFLAN	Air Force LAN
APL	Approved Products List
ASOCNET	Army Special Operations Command Network
ATM	Asynchronous Transfer Mode
BOI	Basis of Issue
BOIP	Basis of Issue Plan
C2	Command and Control
C4	Command, Control, Communications, and Computers
C4I	Command, Control, Communications, Computers, and Intelligence
C4IAS	C4 Intelligence Automation System
CA	Civil Affairs
CIO	Chief Information Officer
CJTF	Combined Joint Task Force (NATO), Commander, Joint Task Force
COE	Common Operating Environment
COMSEC	Communications Security
CONOPS	Concept of Operations
COTS/GOTS	Commercial and Government Off-The-Shelf
CMS	Common Mapping System
CPDB	Command Planning Data Base
CRD	Capstone Requirements Document
DIMHRS	Defense Integrated Military Human Resources System
DIA	Defense Intelligence Agency
DIO	Defensive Information Operations
DJAS	Defense Joint Accounting System
DLA BSM	Defense logistics Agency Business Systems Modernization
DMS	Defense Message System
DNOSC	Deployed Network Operations and Support Center
DODIIS	Department of Defense Intelligence Information System
DPAS	Defense Property Accountability System
ECR	Engineering Change Request
EGP	Exterior Gateway Protocol
ELINT	Electronic Intelligence
EMC	Electromagnetic Compatibility
FCD	Field Computing Device
FOC	Full Operational Capability
GBS	Global Broadcast Service, Global Broadcast System
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GIG	Global Information Grid
GSORTS	GCCS Status of Resources and Training System
GTN	Global Transportation Network
HEMP	High Altitude Electromagnetic Pulse

HCI	Human Computer Interface
IA	Information Assurance
IDM	Information Dissemination Management
IGP	Interior Gateway Protocol
ILS	Integrated Logistics Support
IMINT	Imagery Intelligence
INE	In-Line Network Encryption
IO	Information Operations
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
IT	Information Technology
ITV	In-Transit Visibility
JBS	Joint Base Station
JDISS	Joint Deployable Intelligence Support System
JDST	Joint Decision Support Tools
JIVA	Joint Intelligence Virtual Architecture
JNMS	Joint Network Management System
JOPES	Joint Operational Planning and Execution System
JPAV	Joint Personnel Asset Visibility
JPOTF	Joint Psychological Operations Task Force
JSOTF	Joint Special Operations Task Force
JTA	Joint Technical Architecture
JTAV	Joint Total Asset Visibility
JWICS	Joint Worldwide Intelligence Communications System
KB	Kilobytes
Kbps	Kilobits per second
KPPs	Key Performance Parameters
LAN	Local Area Network
MB	Megabyte
MB	Megabytes per second
Mbps	Megabits per second
METOC	Meteorology and Oceanography
MLS	Multi-level Security
MNS	Mission Needs Statement
MPR&E	Mission Planning, Rehearsal, and Execution
MSE	Mobile Subscriber Equipment
MTBCF	Mean-time Between Critical Failures
NAIC	National Air Intelligence Center
NAVSPECWARCOM	Naval Special Warfare Command
NIE	National Intelligence Estimate
NIPRNET	Non-Secure Internet Protocol Router Network
NRT	Near Real Time
O&M	Operations and Maintenance
CPD	Capabilities Production Document
OSI	Open System Interconnection
OSPF	Open Shortest Path First

PDW	Product Development Workstation
PICRC	Portable Intelligence Collection and Relay Capability
PKI	Public Key Infrastructure
POBS	Psychological Operations Broadcast System
POM	Program Objective Memorandum
RRR	Reliability and Maintainability Rationale Report
PSTN	Public Switched Telephone Network
PSYOP	Psychological Operations
RRR	Reliability and Maintainability Rationale Report
RSP	Readiness Spares Package
SSC-C	SPAWAR Systems Center - Charleston
SIE	SOF Information Enterprise
SIF	SOF Integration Facility
SIGINT	Signal Intelligence
SIPRNET	Secret Internet Protocol Router Network
SLAMS	SOF Logistics and Acquisition Management System
SOCRATES	Special Operations Command Research, Analysis, Threat, and Evaluation System
SOCRATES-D	Special Operations Command Research, Analysis, Threat, and Evaluation System – Deployable
SOF	Special Operations Forces
SOFTACS	SOF Tactical Assured Connectivity System
SOFPARS	SOF Planning and Rehearsal System
SOF-IV(M)	Special Operations Forces Intelligence Vehicle Migration
SOMPE	Special Operations Mission Planning Environment
SOTVS	Special Operations Forces Tactical Video System
STEP	Standardized Tactical Entry Point
STN	Special Tactics Network
TACLAN	Tactical Local Area Network
TCAIMS-II	Transportation Coordinator's Automated Information for Movement System
TDC	Tactical Deployable Communications
TPN	Tactical Packet Network
TBMCS	Theater Battle Management Core Systems
TSOC	Theater Special Operations Commands
TMIP	Theater Medical Information Program
UDA	Urgent Deployment Acquisition
UPS	Uninterrupted Power Source
USSOCOM	United States Special Operations Command
WIN-T	Warfighter Information Network-Terrestrial
WS	Workstation
Y2K	Year 2000

APPENDIX E

Basis of Issue (BOI) and Equipment Replacement Plan

Table E-1 shows workstation Basis of Issue (BOI) by TSOC and Component deployable organization. Table E-2 shows the network packages by Component and Theater SOCs. Table E-3 shows the workstation replacement plan based on a four-year cycle. Table E-4 shows FCD BOI for tactical teams by Component

Table E-1. TACLAN Equipment Basis of Issue
Unit/Organization Totals

Unit/Organization	# of Units	Stand Alone Workstations	NIPR WS	SIPR WS	SCI WS	Coalition WS	SOMPE WS	Total
SOCCENT	4		120	120	40			280
SOCEUR	4		120	120	40			280
SOCJFCOM	1		10[2]	62[2]	10			70
SOCKOR	1		30[2]	60[2]	10			70
SOCPAC	4		120	120	40			280
SOCSOUTH	2		60	60	20			140
TSOC Augmentation	1		30	30	10			70
TSOC Subtotal								**1190-1190=0**
SFOB	7		20	125	12	15		1204
FOB	21		20	75	10	33		2,898
ODB (AOB/SOCCE/ ISOFAC)	63	3	7[2]	7[2]			756[1,4]	1386
SOSCOM FWD	1		25[2]	25[2]			71[1]	96
528 SOSB	1		25[2]	25[2]				25
112th Signal BN	1	20	25[2]	25[2]				45
JPOTF/4TH POG	5		60[2]	60[2]	5			325
JPOTF/2d POG[1]	1		57[2]	275[2]	21	10		306
JPOTF/ 7th POG[1]	1		39[2]	216[2]	13	11		240
96 CA BN	1		65[2]	65[2]	3	47		115
350 CACOM[1]	1		237[2]	365[2]				365
351 CACOM[1]	1		233[2]	360[2]				360
352 CACOM[1]	1		365[2]	584[2]				584
353 CACOM[1]	1		442[2]	723[2]				723
Integration Facility	1		30[2]	30[2]	5	5		40
Training Facility	1		45[2]	45[2]			148	193
Ranger Rgt	1		54[2]	54[2]	15			69
Ranger Bn	3		74[2]	74[2]	5			237
160th SOAR	4		35[2]	35[2]	5			160

Unit/Organization	# of Units	Stand Alone Workstations	NIPR WS	SIPR WS	SCI WS	Coalition WS	SOMPE WS	Total
ARSOF Subtotal								9371-6720=2,651

[1] Workstations included for subordinate units.
[2] Indicates the same workstation will access both NIPRNET and SIPRNET, but with separate hard drives.
[3] Specific unit breakdown in Table E-8
[4] 2 per ODA x 378 ODAs

Unit/Organization	# of Units	Stand Alone Workstations	NIPR WS	SIPR WS	SCI WS	Coalition WS	SOMPE WS	Total
Group 1/2 HQ/Training	2			24				48
Group 3/4 HQ/Training	2			74				74
NACSPEC WARUNIT	5			12				60
TACLAN	7		5	25	10			280
SEAL Team HQ	8			46				368
SDV Team HQ	2			22				44
SBT HQ	3			28				84
NSW Center	1			28				28
SEAL Platoon	56			3				168
MK-V Det (2 craft/MST)	10			4				40
RHIB Det (2 craft)	38			4				150
SOCR Det (2 craft)	10			4				40
SDV Plts	12			6				72
SDV Craft	15			0				0
ASDS Plts	4			4				16
DDS Plts	6			2				12
Program Office	1			8				8
NAVSOF Subtotal[3]								**1522-490=1,032**
AFSOC	2		100	100	15			430
AFSOD	4		60	60	15			540
AFSOE	7		30	30				420
SOLE	4		2	2				16
AFSOC SOMPE [4]							699	699
AFSOF Subtotal Total								**2105-910=1195 4,878**

[3] - NAVSOF plans to use one workstation for multiple LANs (UNCLAS, SECRET, SCI). Multiple removable hard drives will be required.

[4] – AFSOC SOMPE numbers are from tables E-5, 6, 7.

[5] - only 6 segments are required.

Table E-2. TACLAN Network Package Basis of Issue

Unit	UNCLAS	CLASS	SCI
TSOCs			
TSOC *	17 (30 workstations)	17 (60 workstations)	17 (10 workstations)
ARSOF			
SF Group (SFOB)	7 (20 workstations)	7 (125 workstations)	7 (12 workstations)
SF BN (FOB)	21 (20 workstations)	21 (75 workstations)	21 (10 workstations)
PSYOP BN	15 (60 workstations)	15 (60 workstations)	15 (5 workstations)
SOSCOM Fwd SOSB 112th Sig BN	3 (25 workstations)	3 (25 workstations)	0
CA BN	40 (65 workstations)	40 (65 workstations)	1 (5 workstations)
Ranger Rgt	1 (55 workstations)	1 (55 workstations)	1 (15 workstations)
Ranger BN	3 (75 workstations)	3 (75 workstations)	3 (15 workstations)
160th SOAR	4 (35 workstations)	4 (35 workstations)	4 (5 workstations)
Integration Facility and Training	2 (30 workstations)	2 (30 workstations)	1 (5 workstations)
NAVSOF			
TG / TU (Ashore) *	7 (5 workstations)	7 (25 workstations)	7 (10 workstations)
AFSOF			
JSOAC	2 (100 workstations)	2 (100 work stations)	2 (15 workstations)
AFSOD	4 (60 workstations)	4 (60 workstations)	4 (15 Workstations)
AFSOE	7 (30 Workstations)	7 (30 Workstations)	
Total	133	133	83
		Grand Total	133

* The number from Table E-2 reflects increases to BOIP due to Presidential Decision Memorandum 1 2004. This increases SOCCENT, SOCEUR, and SOCPAC to 4 suites allows SOCJFCOM and SOCKOR 1 suite each, SOCSOUTH 2 suites and 112th Signal Battalion 1 suites for augmentation for any contingency.
** These SCI segments will be used by AFSOC to support Intel requirements at whatever level requires them.

Table E-3. USSOCOM Total TACLAN Network Package BOIP Four (4) Year Workstation Replacement Cycle (TBP)
Includes FCDs from Table E-4 below, this table is an *example* only

Organization	FY05	FY06	FY07	FY08	Total
SOCCENT	22	23	23	23	91
SOCEUR	19	19	19	19	76
SOCJFC	20	20	21	21	82
SOCKOR	24	25	25	25	99
SOCPAC	25	25	25	25	100
SOCSOUTH	25	25	25	25	100
TSOC Augmentation	55	55	55	55	220
ARSOF	2,238	2,238	2,238	2,239	8,953*
NAVSOF	428	429	429	429	1,715*
AFSOF	326	327	327	327	1,307*
Totals	**4,814**	**4,813**	**4,814**	**4,813**	**19254**

Workstations and servers will be replaced approximately every four years or when system no longer meets operational requirements. Other peripheral equipment will have a similar replacement schedule based on relative equipment lifecycles. Table 3 shows the anticipated workstation replacement schedule over a four-year period after FOC. Note this table assumes a staggered initial fielding schedule from FY01 through FY04.

Table E-4. TACLAN Field Computing Device (FCD) Basis of Issue

Unit/Organization	Old # of FCDs	New # of FCDs
USASOC	1737	4,032
NAVSPECWARCOM	584	686
AFSOC	188	592
Other	52	450
SOCCENT	5	0
SOCEUR	5	0
SOCJFCOM	5	0
SOCKOR	5	0
SOCPAC	5	42
SOCSOUTH	5	0
Total	**2,242**	**5,802**

- USASOC (Qty: 4,032)
  - 1,764 FCDs for ODA/ODB Teams. 378 ODA teams with 4 FCDs per ODA team (1 per SMRS (2) and 2 for SATCOM data. operations) and 63 ODB Teams with 4 FCDs per ODB Team.
  - 98 FCDs for Group Support Companies (GSC): 7 GSCs with 14 FCDs per GSC. Each GSC has: one Military Intelligence Detachments HQ with 2 FCDs; 42 SOTAs with 1 FCDs per SOTA; one INTERR with 1 FCD; and one CI unit with 1 FCD; one SVCDET with 1 FCD; 1 SIGDET with 3 FCDs.
  - 210 FCDs for Battalion Support Companies (BSC): 21 BSCs with 10 FCDs per BSC. Each BSC contains: 1 SOWT with 1 FCD; 1 MID HQ with 1 FCD; 1 MID with 1 FCD; 1 SVCDET with 1 FCD; and 1 SIGDET with 6 FCDs.
  - 28 FCDs for SFG HHC support: 7 SFG HHCs with 4 FCDs per HHC (1 SOWT with 2 FCDs per SOWT, 1 S6 with 2 FCDs per S6).
  - 285 FCDs for SWCS: one per 18E student radio.
  - 6 FCDs for Battle Lab: development and testing.
  - 1565 FCDs for MBMMR/SATCOM/SMRS Operations for other then ODA/ODB Teams; 1 FCD per MBMMR/SATCOM/SMRS for Rangers (83), PSYOPS (224), CA (1199), SOAR (49), SOSCOM (10).
  - 10 FCDs for SFD-K.
  - 66 USASOC Other

- NAVSPECWARCOM (686)
  - 316 FCDs for NSWG-1/2 SEAL Teams support. Authorized 5 FCDs per Platoon, 7 Platoons per Seal Team, 4 Seal Teams per Group, 2 Groups. (Note: 12 additional SEAL platoons authorized in FY06 and in FY '08. FCD quantities required reflect new SEAL requirements.) 8 SEAL Team HQs x 1 FCD = 8 FCDs. 56 Plts x 5 FCDs each = 280 FCDs. NSWG 1/2 Training 24 FCDs. Group 1/2 HQ Group HQ x 2 each = 4 FCDs. Total for NSWG-1/2 is 316.
  - 243 FCDs for NSWG-3/4. 3 per boat detachment, 3 per Seal Delivery Vehicle (SDV) Platoon, 2 per Special Boat Team Hqs (SBT), 4 per SDV Team HQs. 58 boat Det x 3 FCDs = 173 FCDs, 12 SDV Plt x 3 FCDs = 36 FCDs. 3 SBT x 2 FCD = 6 FCDs. 2 SDV Team Hqs x 4 FCD = 8 FCDs. NSWG-3/4 Training 16 FCDs. Group 3/4 HQ x 2 each = 4 FCDs. Total for NSWG 3/4 is 243.
  - 90 FCDs for NSW Center Courses.
  - 25 FCDs for 5 Forward Units authorized with 5 FCDs per Forward Units = 25 FCDs
  - 12 for NSW TACLAN/SOMPE/FCD Program Office

AFSOC (Qty 592)
  - 342 FCDs for Special Tactics UTCs (1 per operator)
  - 100 FCDs for 24 th STS
  - 29 FCDs for Combat Weather assigned to support Army units.

- 51 FCDs for Communication Flights to support administrative taskings, FAX service, STE data transfers.
- 24 FCDs for Combat Aviation Advisory Teams/FID (24 FCDs to support 8 3-man teams)
- 32 FCDs for Health Services (8 teams at 4 per team)

SOMPE Specific Hardware

TABLE E-5 AFSOC SOMPE Aircraft Systems

Unit	Location	Aircraft Type	Quantity	PAA	Crew Ratio	Notebook
AFSOC						
HQ AFSOC	Hurlburt Field FL					3
CLS Sys Admin Spt	Hurlburt Field FL					4
18 FLTS	Hurlburt Field FL					3
Classified						10
WIC	Hurlburt Field FL					7
TBD		CV-22	50	TBD	2	75
16SOW/XP	Hurlburt Field FL					6
16 OSS	Hurlburt Field FL					4
4 SOS	Hurlburt Field FL	AC-130U	17	14	1.8	55
6 SOS	Hurlburt Field FL		3			3
8 SOS	Duke Field FL	MC-130E	6	4	2	20
9 SOS	Eglin AFB FL	MC-130P	8	8	2	36
15 SOS	Hurlburt Field FL	MC-130H	9	9	1.75	36
16 SOS	Hurlburt Field FL	AC-130H	8	6	1.8	26
19 SOS	Hurlburt Field FL					6
20 SOS	Hurlburt Field FL	MH-53M*	18	18	1.8	36
TBD	TBD	MC-130	13	10	1.75	39
352 OSS	RAF Mildenhall UK					4
7 SOS	RAF Mildenhall UK	MC-130H	5	4	1.75	18
21 SOS	RAF Mildenhall UK	MH-53J*	8	5	1.5	19
67 SOS	RAF Mildenhall UK	MC-130P	5	4	1.5	16
CLS Support	RAF Mildenhall UK					1
353 OSS	Kadena AB Japan					4
1 SOS	Kadena AB Japan	MC-130H	5	4	1.75	18
17 SOS	Kadena AB Japan	MC-130P	5	4	1.5	16
CLS Support	Kadena AB Japan					1
58 TRSS	Kirtland AFB NM					6
550 SOS	Kirtland AFB NM	MC-130H/P	7	7	1.5	25
551 SOS	Kirtland AFB NM	MH-53J*	10	10	1.5	19
CLS Support	Kirtland AFB NM					1

919 OSS	Duke Field FL					6
5 SOS	Eglin AFB FL	MC-130P	5	4	1.5	16
711 SOS	Duke Field FL	MC-130E	8	7	1.5	25
CLS Support	Duke Field FL					1
193 SOG	Harrisburg IAP PA	EC-130	8	7	1.75	28
CLS Support	Harrisburg IAP PA					1
Training at Depot	Hurlburt Field, FL					12
Spares/Unassigned						6
AFSOC Total Reqt			198			612

Table E-6 SOMPE Combat Weather Systems

UNIT	Service	CUST	LOCATION	Req
		TOT PURCHASED:		
		AFSOC TOTALS:		63
AFWA/CWC	N/A	FOR EVALUATION		
HQ AFSOC		AFSOC	HURLBURT	1
720STG/WX	AF	CCT	HURLBURT	1
24STS/WX	AF	24 STS	POPE,NC	3
16OSS/DOW	AF	16SOW	HURLBURT	3
352d OSS/OSW	AF	352dSOG	MILDENHALL, UK	3
353d OSS/OSW	AF	353dSOG	KADENA, JP	3
OL-A, 353 OSS	AF	160th	DEAGU, ROK	2
347th OSS	AF	347th RQW	MOODY, GA	2
HQ 10CWS	AF	4POG	HURLBURT	1
Det 1, 10CWS	AF	1SFG	FT LEWIS, WA	3
	AF			
Det 2, 10CWS	AF	5SFG	FT CAMPBELL, KY	4
	AF	160thSOAR		3
Det 3, 10CWS	AF	10SFG	FT CARSON, CO	3
Det 4, 10CWS	AF	75th RR	FT BENNING, GA	4
Det 5, 10CWS	AF	3SFG	FT BRAGG, NC	4
	AF	7SFG		4
OL-A, 10 CWS	AF	3/160 SOAR	HUNTER AAF, GA	2
OL-A, 320STS	AF	1/1SFG	TORII STN, JP	2
OL-A, 321STS	AF	1/10SFG	PANZER KASERN, GE	2
146WF	ANG	193SOG	HARRISBURG, PA	2

146WF		919SOW		2
146WF		2POG		1
107WF	ANG	20SFG	SELFRIDGE, MI	4
181WF	ANG	19SFG	CARSWELL FLD, TX	4

Table E-7 SOMPE Special Tactics Squadron Systems

UNIT	Service	LOCATION	Req
		AFSOC TOTALS:	**24**
		STOC	**24**
720STG	AF	HURLBURT FIELD FL	
21 STS	AF	POPE AFB,NC	
22 STS	AF	MCCHORD AFB, WA	
23 STS	AF	HURLBURT FIELD FL	
24STS	AF	POPE AFB,NC	
123 STS	ANG	LOUISVILLE, KY	
320 STS	AF	KADENA AB, JP	
321 STS	AF	MILDENHALL, UK	

TABLE E-8 SOMPE Army Ground

Unit	# of Units	Quantity Each	Quantity Projected	PMPS Current	PMPS Projected
SFODA	378	**2**			**756**
JFKSWCS	1	**148**			**148**
SOSCOM	1	**71**			**71**
Totals					**975**

Army Table excludes Ground mission-planning peripheral hardware; this equipment is documented in the SOMPE ORD

Appendix F

Field Computing Device Requirements

The below requirements were identified during the FCD working group held 20 August 2003.

FCD HARDWARE REQUIREMENTS				
REQUIREMENT	USASOC	AFSOC	WARCOM	JSOC
FORM FACTOR 9"W X 7"D	T	T	T	T
Weight (<4 lbs)	T	T	T	T
WIN 2K/XP COMPLIANT	T	T	T	T
1 GB RAM	O	O	O	O
512 mb RAM	T	T	T	T
40 – 80 GB Removable HD (x2) [Shock mounted]	T	T	T	T
User Removable Hard Drive	T	T	T	T
Clamshell	T	T	T	T
Tablet	NA	O	O	
IA compliant PDA type device	O	T		T
Two USB 2.0 ports	T	T	T	T
Four USB 2.0 ports		O	O	
Low Power Mobile Processor	T	T	T	T
Embedded NIC	T	T	T	T
Extended Life (>6 hours) battery	T	T	T	
Extended Life(>8)	O	O	O	T
Color Display	T	T	T	T

Table F-1 FCD Requirements

FCD HARDWARE REQUIREMENTS				
REQUIREMENT	USASOC	AFSOC	WARCOM	JSOC
Embedded 56k Modem	T	T	T	T
Capable of operating with a removable 802.11X Wireless device (PCMCIA)	T	T	T	T
Embedded CF card slot	T	?	T	T
1 x PCMCIA Type II slot	T		T	T
2 PCMCIA Type II Slots		T		T
Audio/Video IO ports	T	T	T	T
Embedded GPS (antenna in screen frame) must be SAASM compliant	O	O	O	O
NVG/Sunlight readable screen	O	O	O	T
IEEE 1394 port (firewire)	O	O	O	O
Roll-up keyboard		O		O
Touchpad/Eraser Head	T	T	T	T
LED Head Mounted Display	O	O		O
33' Depth Transit survivable	O	O	O	O
Serial Connection (DB9)		T		
Environment (meet Commercial Std)	T	T	T	T
Magnesium Alloy (or like) case	T	T	T	T

Table F-1 FCD Requirements

APPENDIX G

Glossary

Bandwidth - The frequency range between the highest and lowest frequencies, expressed in hertz, passed through a network. Bandwidth is divided into smaller frequency ranges, which can be assigned to particular transmission uses.

Capacity - The amounts of communications traffic a circuit, multiplexer, or network system can support. The available bandwidth and the ability to maximize bandwidth use determine capacity.

Client-Server - An architecture for network services in which a central computer (the server) runs programs that provide file storage, electronic mail, data base management, and access to shared resources, while a number of remote user terminals run "client" software designed to access and share these resources.

Configuration Management (CM) - In its purest sense, is a system engineering management process that identifies the functional and physical characteristics of a system during its life cycle; controls changes to those characteristics; and records and reports change processing and implementation status. Configuration management involves four primary functions: identification, control, status accounting, and audits.

Connectivity - The ability to effectively integrate information and communications equipment including equipment with different standards and protocols.

Defense Information Infrastructure (DII) - Resources identified by Defense Information Systems Agency (DISA) as critical for the flow of information within the DOD. Interoperability and multi-path technologies are being applied to the DII to make it as flexible as possible. DISA and NSA are working on multi-level security capability for DII.

Demand Assignment - A feature that is unique to the node that continually optimizes network bandwidth resources. Network resources/bandwidth, are allocated only to active calls. The node monitors signaling from each attached voice or data device, and determines when service is required; only then is bandwidth allocated. Because bandwidth is not wasted on inactive ports, the efficiency of transmission facilities is increased, while reconnecting only active calls optimizes rerouting performance.

Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) - The standard DOD process for identifying information security requirements, providing security solutions, and managing Information Systems (IS) security activities.

Digital Signal - A discrete or continuous signal; one in which various states are identified with discrete levels or values.

Encryption - In security, the ciphering of data by applying an algorithm to plain text in order to convert it to cipher text.

Government Open Systems Interconnection Profile (GOSIP) - A standard for connections between networks adopted by the federal government in 1988, but not widely implemented, due to the large installed base of TCP/IP networks.

Information Superiority - That degree of dominance in the information domain which permits the conduct of operations without effective opposition

Infrastructure - A term generally applicable to all fixed and permanent installations, fabrications, or facilities for the support and control of military forces.

Integrated Service Digital Network (ISDN) - The ISDN is an emerging international standard for public and private networks with the purpose of standardizing protocols and communications networks interfaces, and accommodating mixed transmission services.

Interface - The point between two devices where electrical signals, connectors, timing, and handshaking meet.

Joint Technical Architecture (JTA) - The JTA is a document that identifies a common set of mandatory information technology standards and guidelines to be used in all C4I systems and the interfaces of C4I systems with other key assets.

Local Area Network (LAN) - A type of high-speed data communications architecture where all segments of the transmission medium (typically coaxial cable, twisted-pair wire, or optical fiber) are in an environment under the control of the network operator.

Mean Time Between Failure - This is a stated or published period of time that a user can expect a device to operate before an incapacitating failure occurs.

Middleware - Software that mediates between an application program and a network. It manages the interaction between disparate applications across the heterogeneous computing platforms. The Object Request Broker, software that manages communication between objects, is an example of a middle ware program.

Network - This is a circuit configuration of two or more nodes that interconnects links. A network can have up to 16,000 domains, each including up to 250 nodes, connected in any topology (such as: star, ring, and full mesh).

Network Interface - The point between the carrier's network and the user's installation.

Open Systems Interconnection (OSI) - A top-level model of network architecture that specified seven functional layers: physical link, data link, network, transport, session, presentation, and application.

Operational Environment - A composite of the conditions, circumstances, and influences which affect employment of military forces and bear on unit commander's decisions.

Path - This is the route a call takes through the nodes to reach its destination.

Protocol - This is a formal set of communications conventions and rules setting the format and control of inputs/outputs between two communicating devices or processes. Protocols are typically established by industry organizations: Institute of Electrical and Electronics Engineers (IEEE) or American National Standards Institute (ANSI).

Satellite Communications - This is the use of geostationary orbiting satellites to relay transmissions from one earth station to others for network management.

Special Mission Unit (SMU) - Generic term for designated task organized group of operations and support personnel that performs highly classified activities.

System - Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions.

Telecommunications - This is a term encompassing both voice and data communications in the form of coded signals over media.

Transmission - This is the dispatching of a signal, message, or other form of intelligence by wire, radio, telegraphy, telephony, facsimile, or other means; a series of characters, messages, or blocks including control information and user data.

Transmission Control Protocol/Internet Protocol (TCP/IP) - A widely used set of standards that define the rules for message traffic between networks.

Wide Area Network (WAN) - A group of computers or local area networks connected over relatively long distances to exchange information and share resources