NOAA '95

A Vision For The Future

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 01081995	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Horizons ’95 C4I A Vision for the Future	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Information Assurance Technology Analysis Center (IATAC) 3190 Fairview Park Drive Falls Church VA 22042	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 246	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	8/1/95	Brochure

4. TITLE AND SUBTITLE
Horizons '95 C4I A Vision for the Future

5. FUNDING NUMBERS

6. AUTHOR(S)
U. S. Air Force

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis
Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

The Horizon concept developed in 1993, focused on information architectures and was built as an Air Force (AF) extension of the Joint Staff's C4I for the Warrior construct and defined a path to an AF wide architecture for C4I systems. C4I Horizon '95 expands on this and updates the plan for the 21st Century. The objective is to define the planning perspective and path for information systems and the application of technology across the spectrum of AF operations.

14. SUBJECT TERMS
C2C3C4

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

FROM THE CSAF

Washington, DC – August 1995

The world is entering an age where knowledge, technology, and economic wealth often coalesce to form information power bases. In fact, information is becoming a new center of gravity – a strategic asset, inviting attack and requiring protection. In the past, warfare has been described in four operational environments: air, land, sea, and space. Now, *information* is recognized as the *fifth* operational environment, and information dominance across the spectrum of conflict is crucial to military success.

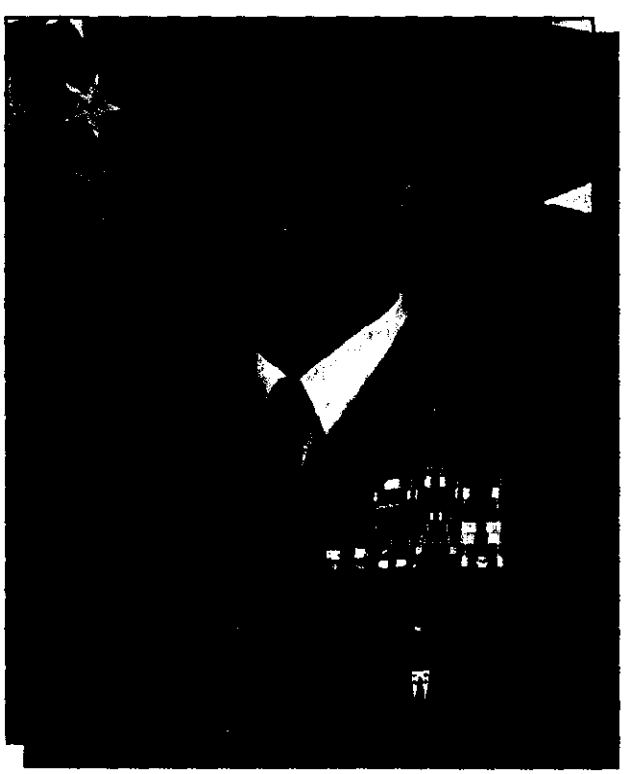
The conflicts in Southwest Asia, Somalia, Bosnia and Haiti have shown that information technology has significantly altered traditional concepts for military operations. That same technology is improving our situational awareness on a global scale and augmenting our ability to generate military options before crises erupt. Once military force becomes necessary, information technology provides numerous options for prosecuting the conflict.

In recognition of the importance of information technology for the Air Force, the HORIZON concept was developed in 1993. That first version of HORIZON focused on information architectures by advancing a vision of an integrated and responsive global infosphere supporting *Global Reach, Global Power* objectives. HORIZON was built as an Air Force extension of the Joint Staff's *C4I for the Warrior* construct for joint interoperability and sought to define, for the first time, a path to an Air Force-wide architecture for C4I systems. That objective has been substantially achieved, and it is now time to update the HORIZON document.

This updated edition, C4I HORIZON '95, expands upon the original by establishing 21st century Air Force information infrastructure objectives, and by planning for rapid integration of evolving technology with the current and future infrastructure. In addition to *enabling* all military pursuits, information-related activities will transcend all we do in air, land, sea, or space operations. They will also enable the concept of *Global Awareness*.

History has shown that the side that effectively analyzes, decides, and acts the fastest will prevail in any conflict. We can and must make optimum use of information technology to operate inside any opponent's decision cycle. That requires unequivocal dominance of the infosphere. The notion of a global infosphere is ambitious; but the future of our Air Force and the defense of our nation depend upon vigorous pursuit of the HORIZON vision by all commands, agencies, and functional domains.

RONALD R. FOGLEMAN, General, USAF
Chief of Staff



INTRODUCTION:

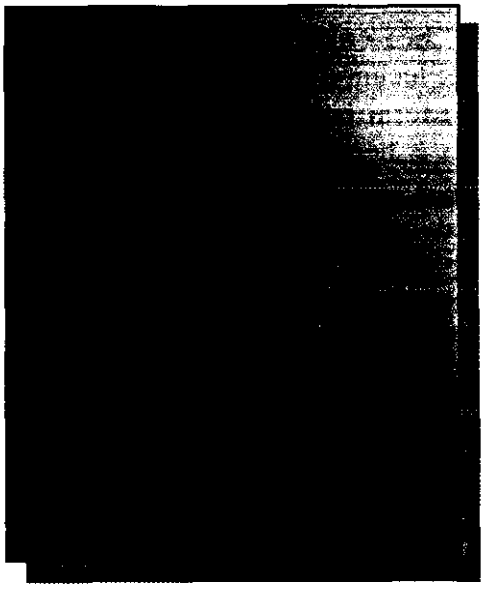
As the Air Force approaches the 21st century, its dependence upon, and its ability to use, information technology grow rapidly. Air Force doctrine is beginning to reflect on the implications of information as an element of combat operations. The concepts of offensive and defensive information warfare and modeling and simulation have gained increased emphasis in doctrinal discussion.

Commercial technology trends and their implications for the future of Air Force operations are only vaguely understood. Most leaders, planners, and doctrinal thinkers share a growing awareness of the importance of the technological changes taking place and are eager to posture the Air Force to meet and defeat likely threats to national interests in the coming millennium. Yet, it is difficult to reach a consensus on either the threats or the potential responses in the near term.

Technology advances that used to take months, years, even *centuries*, now occur almost daily. It is easier to project advances in the rate-of-change than it is to forecast the products of such advances or their implications for the Air Force.

Several major initiatives must be undertaken if the Air Force is to fully benefit from the application of information technology and evolve into the premier combat force of the information age. The preliminary road map for such efforts was laid out in the 1993 edition of HORIZON. This new edition is intended to expand that message, make it more comprehensive, and better articulate the path for its implementation.

C4I HORIZON '95 is a multifaceted concept. It is a vision for achieving information superiority and for leading the Air Force into the information age. The principal objective is to define the planning perspective and evolutionary path for information systems and the application of information technology across the spectrum of Air Force operations. The Air Force cannot — must not — do this alone. This new HORIZON is



intended to provide the path to integrate Air Force C4I systems and services with those evolving in the joint services' areas of operation.

The future of the Air Force depends upon its ability to solidify, implement, and sustain a comprehensive, globally pervasive architecture for the reliable, secure exchange and processing of information at every level of operation. It is essential that this architecture encompass not only command, control, and intelligence information — the traditional operational tools of decision makers — but also modeling and simulation, the virtual battle space, and the myriad personnel, medical, logistical, and other functional area information requirements.

The next 5 to 10 years will see enormous advances in technology domains of importance to the Air Force. HORIZON must lead the way to modernize Air Force infrastructures to secure the advantages new technologies bring. Without such a vision, and in the absence of the resultant infrastructure, optimum use of the newest technologies will remain beyond the reach of the warrior and decision maker.

SETTING THE VISION:

A credible vision for the future recognizes the central importance of information technology and information-related services, systems, and capabilities. The future of the Air Force depends heavily upon a flexible infrastructure to easily and quickly incorporate technological advances from the marketplace. This capability provides the war fighter with the necessary knowledge for any decision, mission, or purpose, whenever and wherever demanded.

Achieving these objectives will be challenging. Rapid technological advances can exacerbate old and introduce new interoperability problems. Antiquated federal and state statutes, the lack of a global vision on the part of information transfer providers (both commercial and military), unfriendly interfaces between people and computers, and inadequate information protection methods and tools can delay progress. Although OSD has mandated that all migration systems conform to the DoD Technical Architecture Framework for Information Management (TAFIM), that stipulation does not guarantee interoperability among rapidly changing systems because some TAFIM standards lack consistency. An Air Force-wide information system architecture is needed to coordinate the diverse system migration strategies of Air Force major commands (MAJCOMs) and to smooth the introduction of new technologies into the Air Force and DoD. State-of-the-art information technology can be integrated with Air Force systems. To enable the defense "...of the United States through the control and exploitation of air and space," the Air Force C4I community must:

[redacted]

The concept of HORIZON was derived from this C4I mission. HORIZON is the Air Force vision for achieving global preeminence in the derivation, management, and integration of information architectures; in the rapid recognition, assessment, and

application of new information technology; and in the visualization, evolution, and utilization of a joint, integrated global information transfer medium — the global infosphere.

Shaping the future battle space is fundamental to HORIZON. While forecasting the future is complicated by the increasing rate of change in world affairs, culture, environment, and technology, it is, nonetheless, essential. Forecasting forms the HORIZON perspective. Essential elements of the process are displayed in Figure 1. Sources for HORIZON planning include the 1995 Air Force Scientific Advisory Board *New World Vistas* study, technology developments from both the public and private sectors; lessons learned from operational experience, exercises, and joint demonstrations; and the frameworks generated by interaction with the other military Services, the Joint Staff, and other government agencies. Underlying the HORIZON vision is HORIZON Link, a powerful tool set that supports the development, integration, and analysis of a diverse set of complex information system architectures and migration system development strategies.

Key to the HORIZON construct has been a series of Air Force *Summits* conducted in the 1992-95 timeframe. These summits involved senior leadership discussions and analyses of C4I, Information Warfare, and Modeling and Simulation, and led to significant adjustments across the Air Force.

Figure 1.

Emerging Air Force doctrine acknowledges information as a "fifth operational environment" of warfare. This elevates the importance of improving the flexibility, adaptability, and interoperability of Air Force information systems and integrating the latest information technology into Air Force systems by leveraging state-of-the-art commercial technologies.

HORIZON articulates the necessity to exploit technology and provides the vision, core architecture, and essential impetus for collective management and commercial development of the global infosphere. The HORIZON vision is:

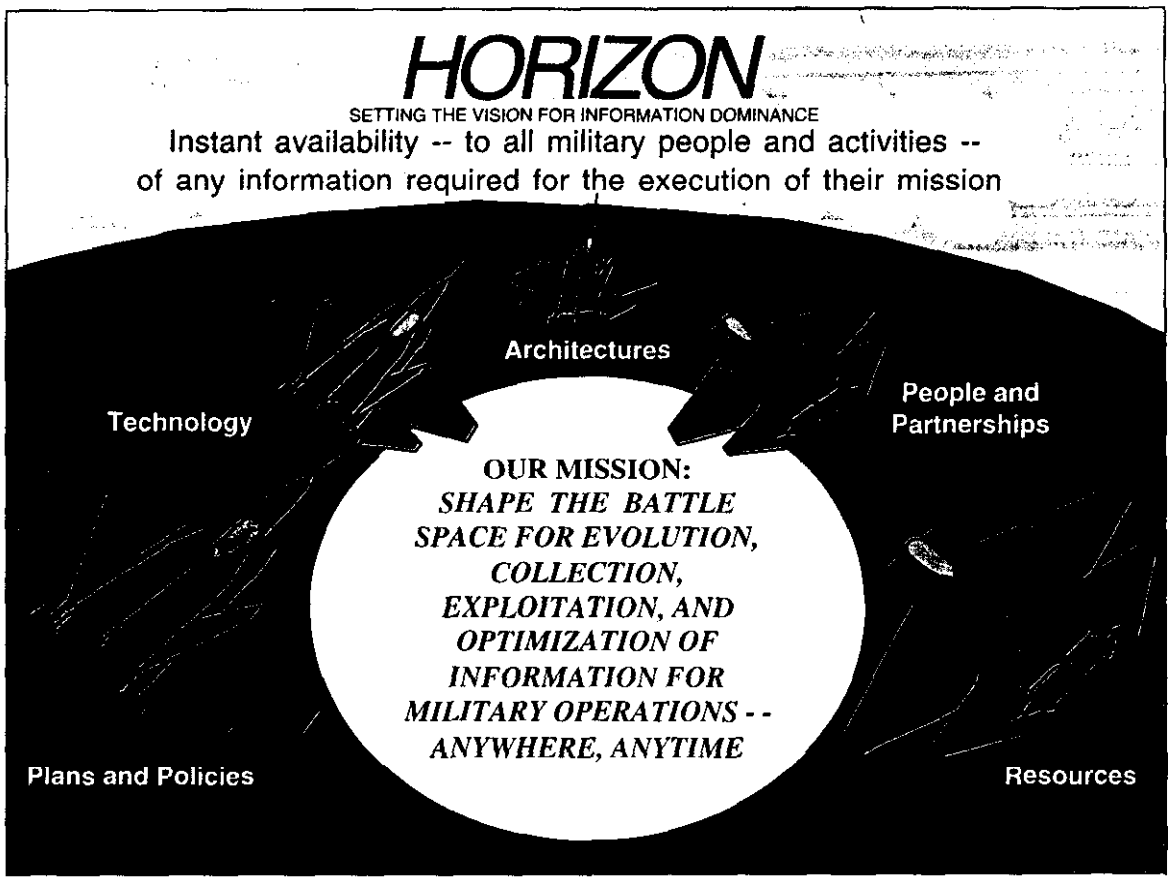


Figure 2.

Figure 2 depicts the constituent parts of the HORIZON concept that will be achieved through compliance with a standards-based information architecture, rapid assimilation of technology, common sense plans and policies, high-quality people looking toward the future, and sound resource management.

HORIZON sets the vision for information dominance – the superior situational awareness applied to seize and maintain the initiative, to shape the enemy's actions, and degrade the adversary's operational effectiveness while denying their ability to do the same.

The HORIZON vision of seamlessly integrated information systems requires an Air Force-wide framework for coordinating and integrating related MAJCOM information architectures. That framework, described in more detail below, has as its foundation a common set of methods, nomenclature, and tools to support the architecture development process.

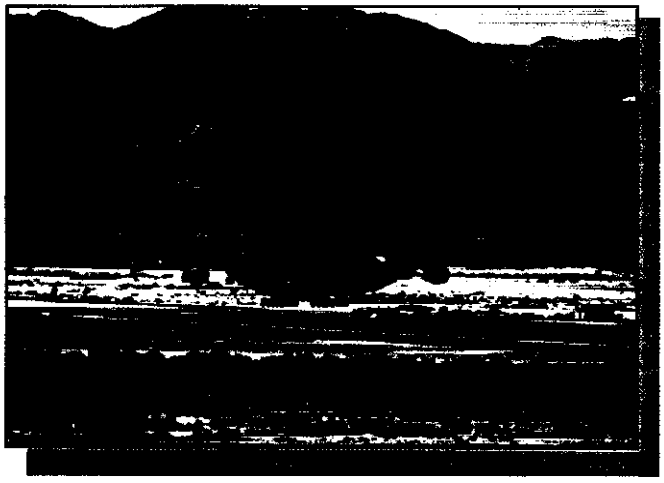
Architectures enable analysis of the performance and interoperability requirements for systems that process and transfer information and facilitate interoperability of Air Force systems with their joint and coalition counterparts. Architectures must be developed to address current and potential future missions and form the basis of analysis in terms of "as is" and "to be" system flexibility, maintainability, cost, and operational effectiveness.

The Defense Science Board has defined three broad constructs as essential to addressing information requirements and planning: operational, technical, and system architectures. The Air Force has adopted these constructs as the foundation of its architecture.

The operational architecture reflects the users' activities. They describe the organizational entities, the business rules they employ, and who talks to whom and the information they exchange, including performance aspects such as volume, timeliness, and sensitivity. Such architectures can be diagrammed in many ways. A rigorous modeling process and notation are essential to capture the functional activities, data, and rules that compose an operational architecture. Functional and data models, including standard data elements, support process improvement and the development of successful automated system solutions.

Technical architectures provide a technical framework, and a minimal set of rules from which automated systems can be developed. They are analogous to building codes for homes, providing guidance on how to build, not what to build. Technical architectures facilitate interoperability by promoting standards and common interfaces. The TAFIM provides overarching guidance on developing technical architectures.

System architectures describe the fielded automated system. They focus on the physical nodes and linkages represented by facilities, sensors, communications, or hardware and software systems. The description identifies all system elements and provides performance specifications (such as bandwidth), electrical interfaces, and hardware and software specifications.



HORIZON Architecture Management Process - The HORIZON information capabilities planning process links operational needs to architectures. In addition to building and managing the architectural framework, the process provides a top-level, enterprise-wide view of the Air Force that enables C4I architects to address hardware and software interoperability requirements and issues. Automated tools are used to display, analyze, and manage key architectural elements and interconnections within the Air Force and between it and other DoD organizations and coalition partners. This tool set permits easy expansion of any area to display greater detail and highlight interconnections among the many mission and support domains inherent to the architecture. Figure 3 is a representation of the HORIZON architecture management process as currently employed.

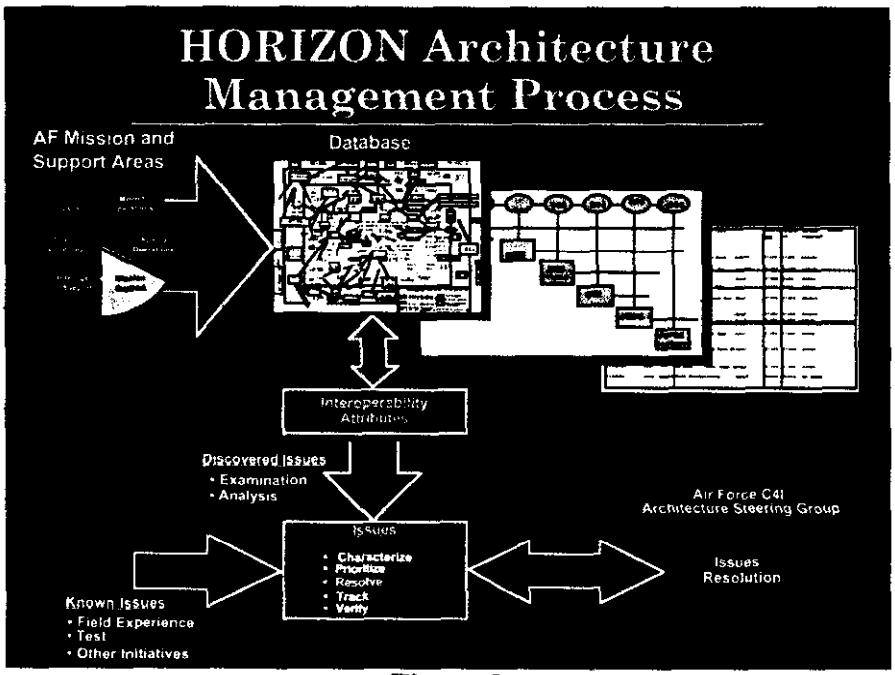


Figure 3.

The HORIZON database used to generate the top-level, Air Force-wide architecture depends on information gathered from specific functional domain architectures. Currently, these data must be extracted from MAJCOM or agency tools and databases and entered manually into the HORIZON database. In the future, automated links will be established between the HORIZON database and the databases and tools used in MAJCOM architectural activities. This will automate updates to the HORIZON database.

Emerging modeling and simulation capabilities also facilitate analysis of information capabilities within the C4I architectural framework. Simulations permit the evaluation of system responses to stress, mission changes, and technology advances. Architects can generate "virtual" environments comparable to simulations used by weapon systems engineers. Gaps in coverage or performance identified through modeling and simulation then translate into future requirements. Simulations, supported by a strong architectural framework, are the means by which information requirements are defined and prioritized and their solutions advocated, implemented, and delivered to warriors in time to take advantage of evolving technology.

Air Force Technical Architecture - Of central importance to realizing the HORIZON vision is the Air Force Technical Architecture. It forms the foundation for information transfer and processing within the Air Force and is essential to system interoperability. It provides a framework of rules, constraints, and attributes for assuring information flows as needed, where needed.

The Technical Reference Codes (TRCs) in the Technical Architecture are derived from the TAFIM, which provides standards profiles, design concepts, components, and configurations to guide development of technical architectures. New technologies are constantly being introduced by commercial vendors, who establish *de facto* or market standards with their new products. TRCs supplement and implement the TAFIM within the Air Force, providing specific guidance and, in certain instances, filling gaps.

The Air Force Technical Architecture will be used to coordinate the diverse migration system strategies developed by Air Force MAJCOMs and to manage the introduction of new technologies into the Air Force. Having a single Air Force Technical Architecture does not imply that all Air Force information systems must be based on the same standards profile. Different organizations have different information processing requirements that may drive different technology and system solutions. However, all Air Force standards profiles or common operating environments must be incorporated into the Air Force Technical Architecture to guarantee interoperability between Air Force information systems and to define and develop any needed data translation or data transfer capabilities. The Army and Navy have also established service-wide technical architectures to ensure interoperability between their own information systems.

Codes, Permits, and Inspections - Institutionalizing C4I Codes, Permits, and Inspections (CPI) ensures C4I capabilities and architectures are used throughout the requirements, acquisition, and test and evaluation processes, thus facilitating their implementation as depicted in Figure 4. CPI provides the necessary policy framework to guide system acquisition and to ensure that individual systems conform to the Air Force Technical Architecture, the TAFIM, and DoD data element standardization (codes). CPI is being implemented as part of the existing program oversight and interoperability certification processes; hence it is not necessary to add overhead to programs for this purpose.

Interoperability begins with a joint review of C4I requirements. These are documented in the Mission Needs Statement, Operational Requirements Document,

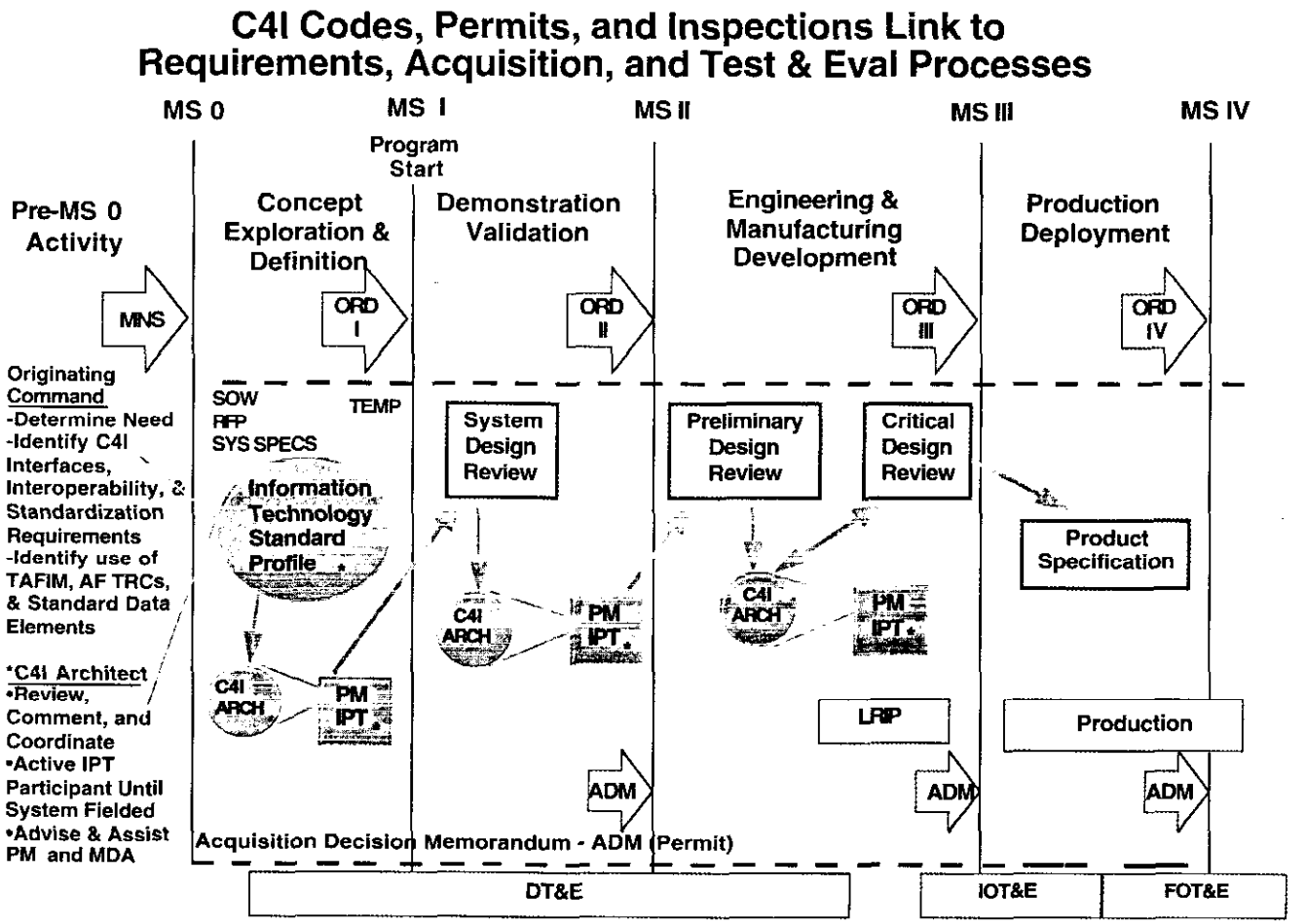
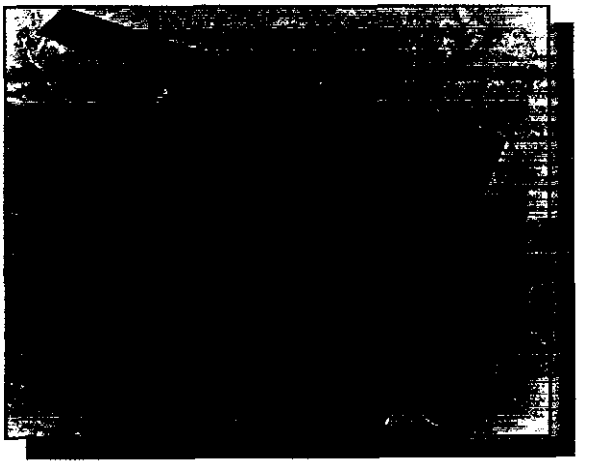


Figure 4.

HORIZON planners envision the war fighter exercising command and control using a common operating environment of distributed, collaborative planning and smart push/pull information facilities. This environment will be as transparent to the user as the electrical power distribution system is to its customers today. Knowledge-based C4I systems will foster the ability to "push" designated information to the user while simultaneously permitting the user to "pull" additional information as required.

The information appliance of the future will be a missile, an F-22, a tank, a land mine, and the shipping pallet used in a deployment. Such appliances will use the global infosphere for sharing information such as location, target, weather conditions, contents, and altitude. The challenge will be to intelligently process this information. Computer chips capable of matching the human brain's processing capability and 3-D optical storage will become commonplace. Intelligent systems will provide expertise at every echelon of command. Miniaturized information appliances able to satisfy both in-garrison and field operations will enhance the ease and speed of deployment and provide the means for true "train as you fight" capability. Personal communications devices will provide real-time, multimedia connectivity, and directly interface to every required information source, such as the Global Positioning System and the Global Command and Control System.



In the absence of information dominance, air, land, sea, and space operations are significantly more vulnerable to crippling losses and disruption. Due to its increased reliance on information systems, the United States is extremely vulnerable to the threats posed by information warfare. In response, the Air Force is developing a strategy for information protection. That strategy prescribes an integrated risk management approach employing appropriate elements of operations, communications, information, emission, and computer security. The information protection process establishes a baseline of critical data and essential networks and systems and assesses their vulnerability to determine appropriate protection based on operational priorities while considering economies of scale.

An integrated, protected, joint information system architecture provides an efficient framework for applying advanced technologies. The 21st century *information warrior* must ensure advanced technology applications are easily exploited and integrated within the infosphere. Universally interoperable, highly flexible hardware and software will provide ready capacity to interface and exchange data with other Services and allies. This sharing of information, coupled with faster, smarter machines, will result in exponential improvements in combat capability and reduce the decision cycle for the war fighter. Bandwidth-on-demand and a global network will eliminate the familiar communications gridlock of today, providing immediate connectivity and an uninhibited flow of information to everyone - from the airman ordering jet engine parts to members of the National Command Authority.

The National Military Strategy establishes requirements for a secure, interoperable, network-of-networks as the overarching DoD information systems programming objective. The Joint Staff's *C4I for the Warrior* outlines a strategy focusing on unity-of-effort across the DoD. Air Force strategies delineate the operating parameters for an information environment optimized for projection of air and space power. HORIZON assimilates the tenets of the Joint Staff's *C4I for the Warrior* and the Air Force themes of *Global Awareness, Reach, and Power* to guide a hierarchy of planning activities supporting information-based combat and other real-time decision support.

The long-term objective of the HORIZON plan hierarchy is to produce an environment enabling the situational awareness, strategic agility, and lethality essential to the *Global Awareness* concept. As depicted in Figure 5 and defined in Table 1, a hierarchy of interrelated planning documents provides the muscle and sinew to support the HORIZON vision.

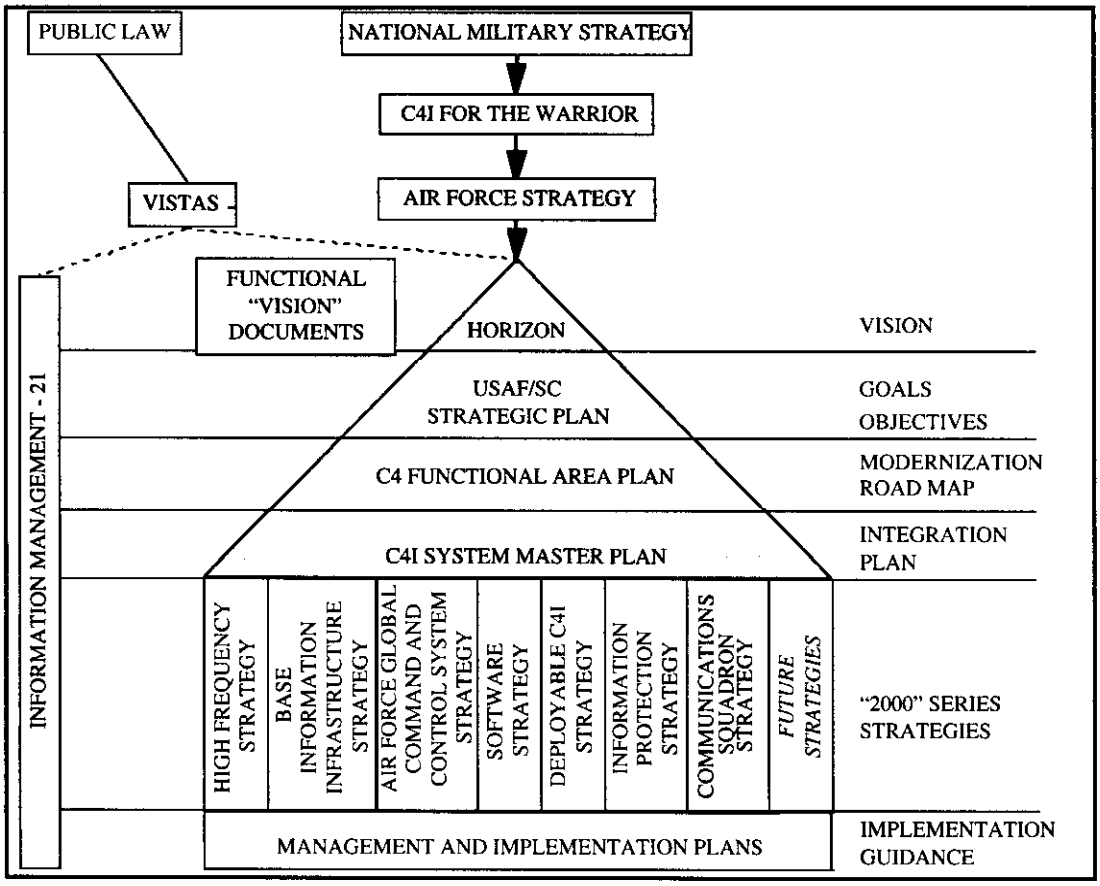


Figure 5.

HORIZON Plan Hierarchy

Δ *HORIZON*: Sets the Air Force vision for application of information technology to achieve instant availability of information. Responds to information needs envisioned by all mission and functional areas.

Δ *Sentinel - The Air Force Intelligence Strategic Plan*: Provides core values, vision, mission, and goals for Air Force Intelligence.

Δ *USAF/SC Strategic Plan*: Charts the course to the HORIZON vision through goals and objectives.

Δ *VISTAS - Information Resource Management Strategic Plan*: Establishes the overarching, corporate Air Force direction for information resources management.

Δ *C4 Functional Area Plan (FAP)*: Integrates visionary applications of technology into a 25-year road map to deliver complete C4I system capability for warriors and other decision makers.

Δ *C4I Systems Master Plan (C4ISMP)*: Synchronizes information-based programs and initiatives to assure successful attainment of HORIZON goals and objectives.

Δ *"2000" Series Strategies*: Outline improvement strategies for the constituent parts of the Air Force information enterprise.

Δ *Implementation Guidance*: Supports each strategy with appropriate management and implementation plans for specific information systems or capabilities.

Δ *Information Management 21 Plan*: Provides a comprehensive road map for managing the growing volume of Air Force information, with emphasis on functional process improvement.

Table 1.

Policy changes needed to achieve the goals articulated in *C4I for the Warrior* and the Air Force themes of *Global Awareness, Reach, and Power* are summarized in Table 2.

Policy Solutions to Architecture and Implementation Assessment Issues	
Improved coordination of Air Force architecture activities	• Establish a consensus-based policy for joint coordination of DoD architecture efforts • Set methodologies, tools, and information standards for Air Force architectures
Effective Air Force Technical Architecture (AFTA) policy framework	• Establish design authority for AFTA • Establish core set of mandatory TRCs • Establish AFTA enforcement authority
Improved interoperability assessment capabilities	• Collect and synthesize data from exercises • Link MAJCOM architecture tools and data with HORIZON database
Policy Solutions to Migration Systems Issues	
Air Force and DoD migration system interoperability	• Coordinate AFTA and migration profiles • Define potential gateway, translation needs • Create conformance metrics for migration systems
Technology insertion coordination	• Track and assess net technologies early
Policy Solutions to Data Standardization Issues	
Coordination of MAJCOM data standardization submissions Improved MAJCOM technical support Data standardization for migration systems	• Clarify, extend, and strengthen Air Force data standardization policy - include migration system guidance - establish Air Force data model clearinghouse - create uniform contract guidance • Establish Integrated Product Teams • Continue MAJCOM training by AFC4A • Incorporate improved Air Force Data Administration program in HORIZON

Table 2.

These measures have been organized into an achievable plan, to be executed in three phases as shown in Figure 6. In the first phase, a uniform architecture development framework will be established throughout the Air Force. Architectural tools and data developed by different Air Force organizations will be linked by a secure connection to the HORIZON database. In the second phase, an improved Air Force data standardization program will be implemented that includes relevant measures outlined in Table 2. In the third phase, design and enforcement responsibilities for the Air Force Technical Architecture will be established along with a core set of codes for all Air Force C4I system development programs.

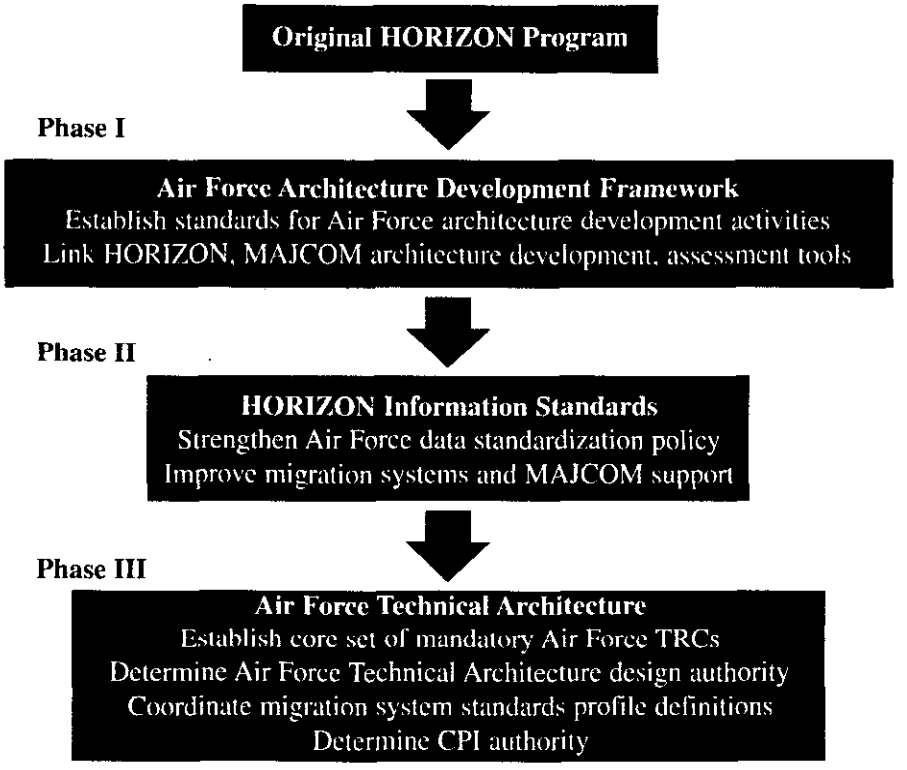


Figure 6.

PEOPLE AND PARTNERSHIPS:

As information becomes increasingly integrated with modern warfare, highly trained information warriors and partnerships between the military and industry are key to achieving information dominance.

Corporate commitment within the DoD and external ties to industry are required to develop, implement, and maintain the capabilities needed to succeed in the information-based warfare environment. Only an internal DoD partnership will produce the seamless, common operational environment required to conduct joint operations. Incorporating Air Force C4I professionals into operational units as "crew members" will promote the necessary expertise to rapidly exploit technological advances.

Partnerships with industry are necessary to take advantage of the national industrial base and to meet military "surge" requirements. Industry should be encouraged to develop innovative information technologies. Low-risk demonstrations allow the war fighter to test new technologies in an "operational" environment. Free of formal development testing and certification requirements, these demonstrations enable the military to preview commercially available, leading-edge technology and rapidly insert it into operation. Keeping industry apprised of important military concerns through continual exchange of information can improve Air Force leverage in technology development and simplify the integration of new technology into military systems.

With the information age, expeditionary warfare takes on a new element — *information operations*. In this environment, the information warrior must be able to "unplug" that portion of the modular garrison information system needed for field operation, deploy

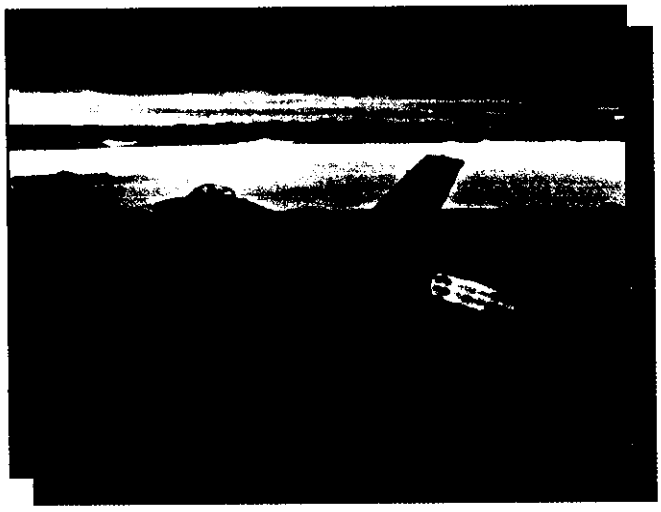
with the combat wing, "plug in" to joint/coalition networks in the theater, access the infosphere, and provide the commander with real-time information on demand. Modular C4I elements must be fielded to allow use of the same screens and information, equipment, people, and procedures in deployment as at home. The information warrior must also be prepared to "virtually" project combat presence to all parts of the globe without leaving home base.

The Air Force must educate and train its people in the philosophy, doctrine, and techniques of air, space, and information operations. C4I professional and technical training must also focus on information warfare, information management, and system and network design, engineering, and management. The result will be C4I professionals with the expertise to plan, design, develop, implement, operate, and maintain requisite information capabilities for all operational and support activities.

The partnerships to exploit information technology — and highly competent personnel to employ those technologies — will create a team capable of fighting the information battle. The air commander needs to control the battle space — air, space, and information. Information technology can become a first-use weapon to deter or compel, a combat weapon added to the Air Force arsenal, and the ultimate weapon to help defeat any enemy. This reality necessitates appropriate resource planning and allocation to ensure development, acquisition, and fielding of the technology needed to project presence.

RESOURCES:

The Air Force recognizes information and information functions as lucrative targets — valuable resources worthy of vigilant defenses — and a realm within which military operations are conducted. To achieve superiority in this new operational environment, commitment is required by all echelons of command to field new technologies, provide training, and develop the required support structure. A complete overhaul of



the base and airborne information infrastructure, integration of information protection tools, and acquisition of modern theater deployable communications are required to achieve the vision set forth in HORIZON. A preparatory step essential for the Air Force to take advantage of new information technology is the Super Highway 2000 initiative and its Program Objectives Memorandum companion, Base Information Infrastructure. These initiatives constitute the first recognition by the Air Force that wide bandwidth inter- and intra-base connectivity are absolutely critical to the Air Force mission. Also essential to our fixed and deployed forces are modernization programs such as Contingency Theater Automated Planning System, Base Level Systems Modernization, Wing Command and Control System, and the Defense Message System-Air Force.

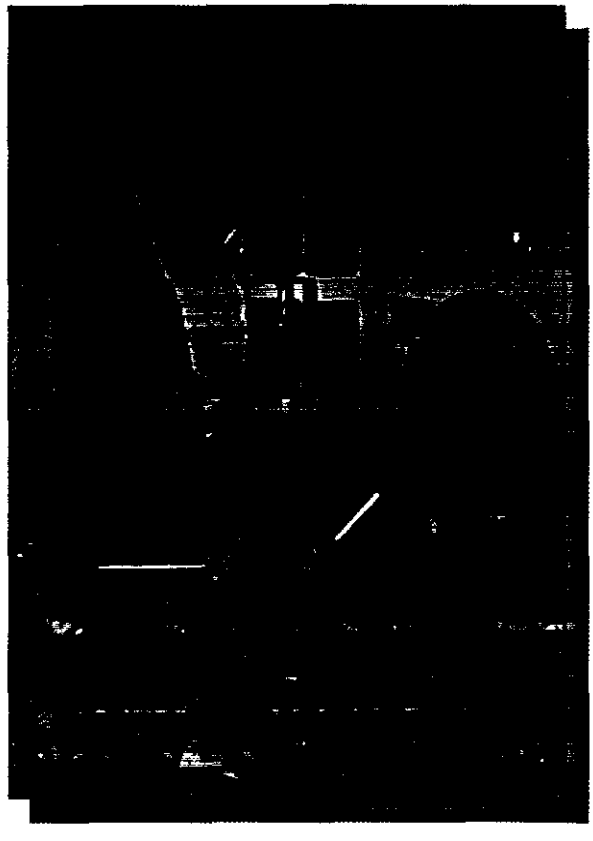
Technological advances, shrinking defense budgets, and force reductions dictate the need to incorporate high-leverage information technology into every aspect of military operations. Through the employment of these technologies, the Air Force can substantially compensate for a smaller force while maintaining a decisive military advantage. The most advanced technologies, the most dynamic plans, the clearest policies, and the most comprehensive architectures are dependent upon the availability of resources. Money, people, facilities, and technical tools must be available. Therefore, funding strategies must be reassessed. The role and importance of information as a weapon of war dictates funding prioritization on a par with traditional weapon systems.

CONCLUSION:

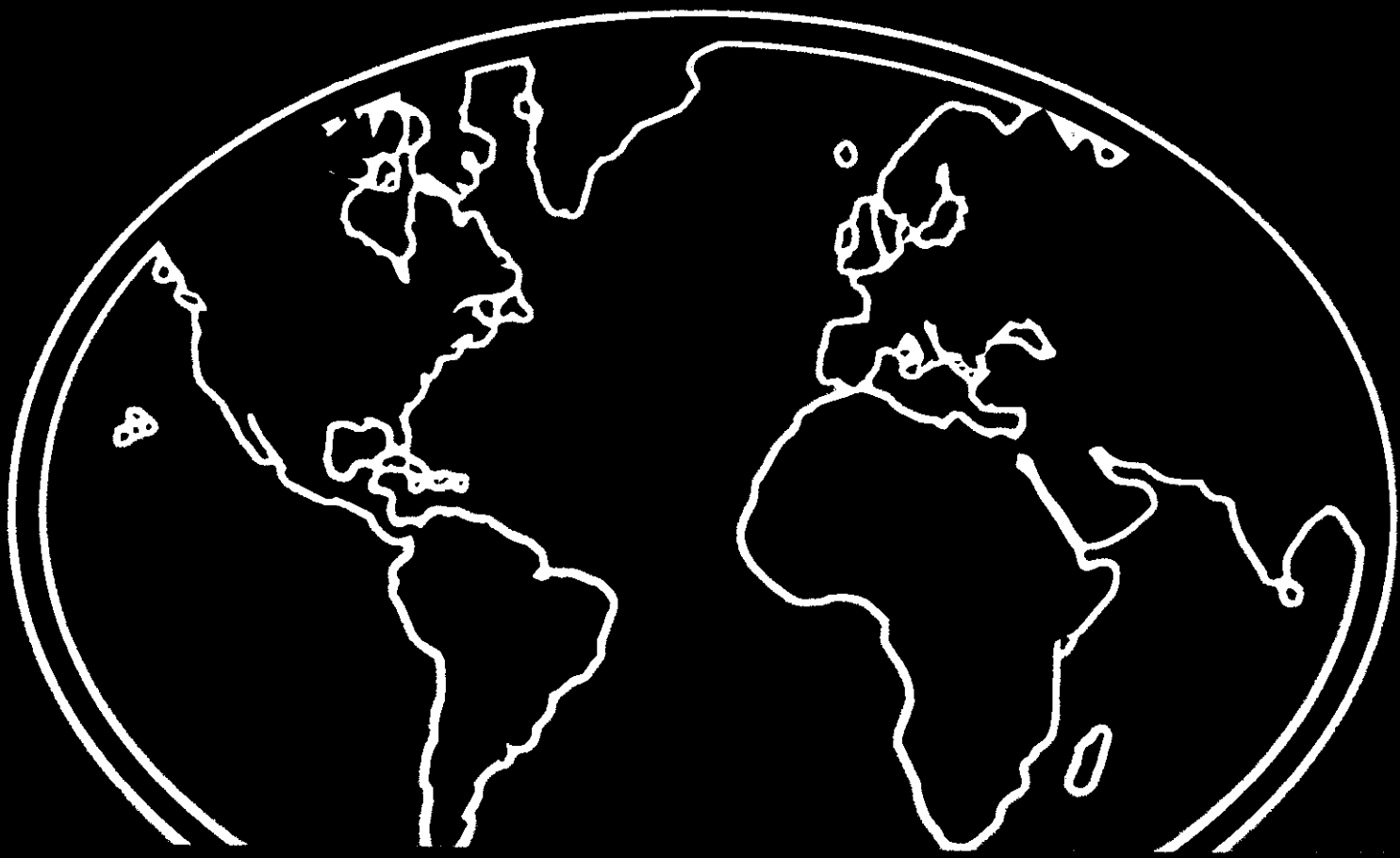
The vision is clear: migration to a single, integrated, and interoperable joint information system providing *instant availability — to all military people and activities — of any information required for, and during, mission execution.*

The war fighter in the 21st century must have unequivocal situational awareness. Such capability demands information dominance in the battle space and secure, reliable, and timely availability of all-source information for decision making. Exploitation and optimization of information technology are paramount to achieving this dominance, and information operations will be the vehicle to achieve and sustain that purpose. Integrated, interoperable C4I systems are the tools required, and effective pursuit of such objectives requires dynamic *plans and policies* to chart the course, *architectures and standards* to establish the framework, *people and partnerships* to form the team, and *resource management* to provide the capability to integrate new *information technologies* throughout the Air Force and the joint community.

To fully exploit capabilities of a much smaller military to execute *Global Awareness, Reach, and Power* requires continuous improvement of C4I capabilities. Information dominance is the goal — information technology is the weapon — integrated, interoperable C4I systems are the means.



C4I



Air Force Deputy Chief of Staff,
Command, Control, Communications and Computers
Policy and Strategy Division
The Pentagon
Washington, D.C. 20330-1250

and C4 Systems Requirements Documents. The Integrated Product Team of users, developers, testers, and architects must ensure interoperability is incorporated early into system design. Active participation by C4I architects enables interoperability and code compliance to be validated (permit) at the various design reviews (inspections) — System, Preliminary, and Critical — as part of program oversight by the appropriate Milestone Decision Authority. From these requirements, the Test and Evaluation Master Plan is built. From this overall process, the Critical Technical Parameters used in Developmental Test and Evaluation and the Critical Operational Issues used in Operational Test and Evaluation are created and used to conduct system testing. Interoperability requirements are validated and certified through integration of CPI with the requirements, acquisition, and test and evaluation processes.

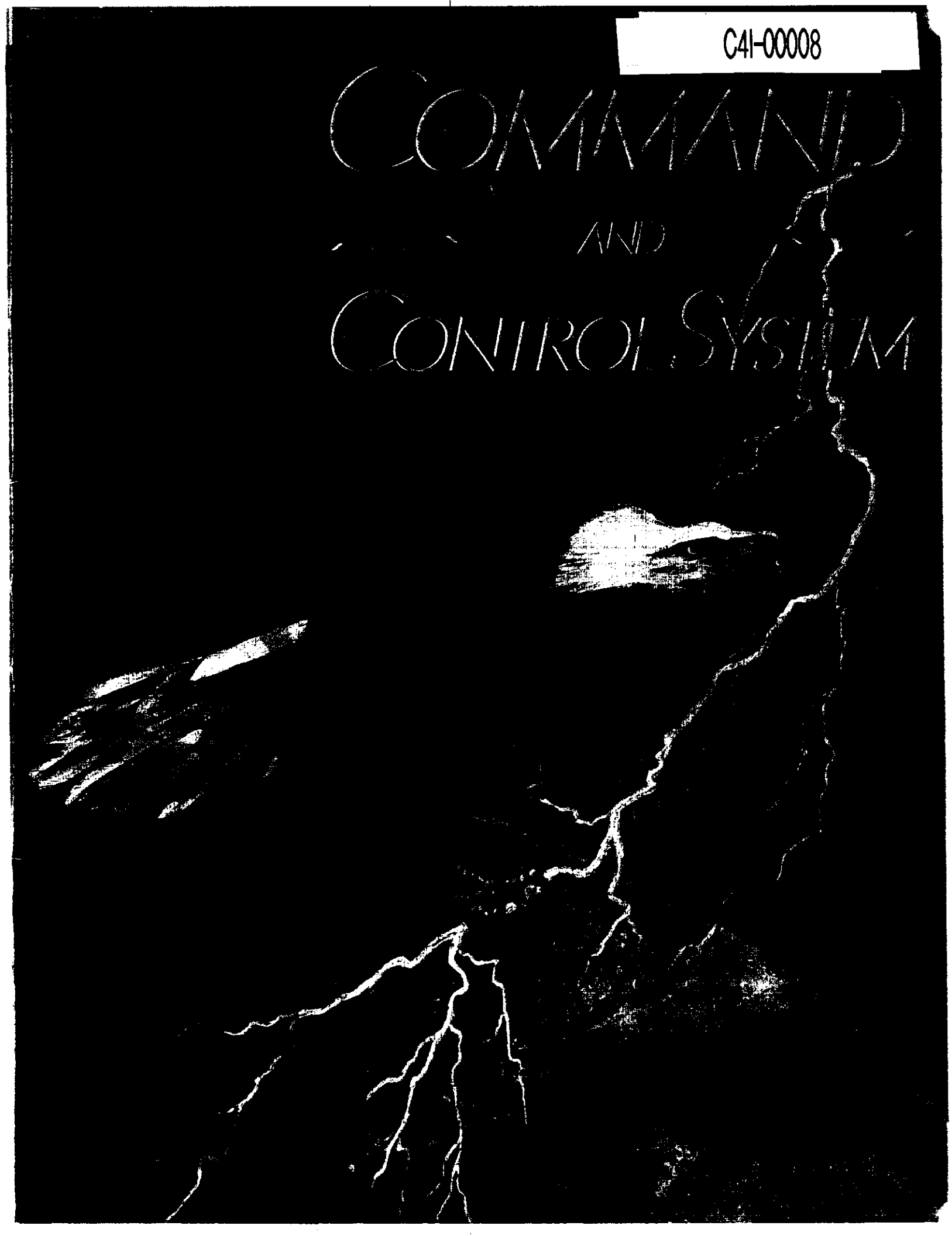
CPI also provides standards to guide Air Force personnel and organizations involved in planning, designing, developing, testing, and fielding ground, air, and space C4I systems. CPI will provide the needed coordination for melding the products of all Air Force information systems programs into a single, seamless, system-of-systems architecture.

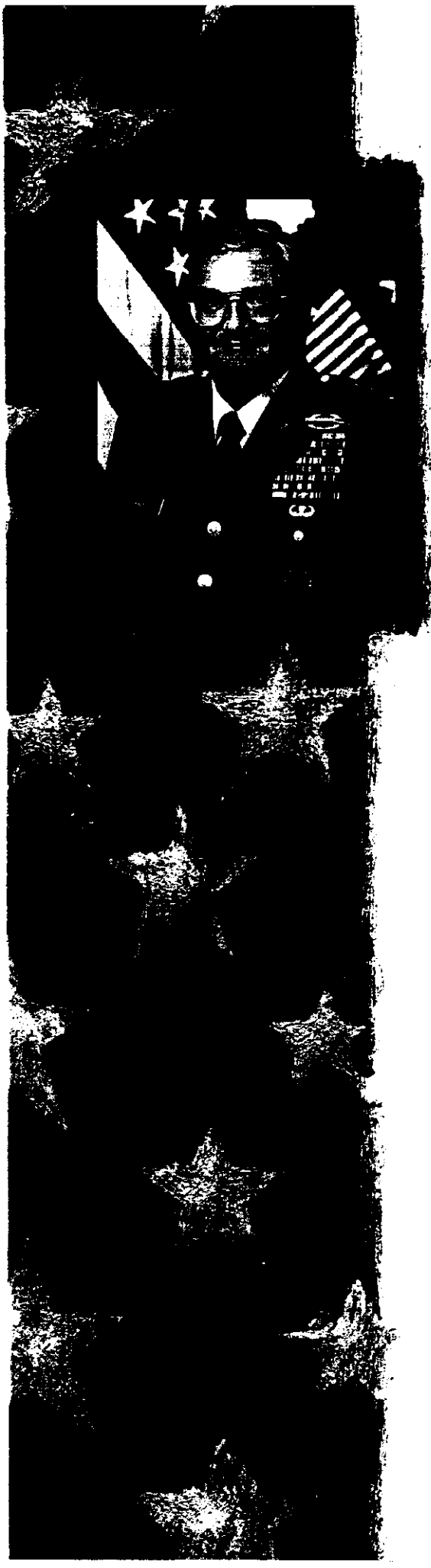
The architectural approach is essential for the software component of C4I. CPI will ensure interoperability by relying on a core set of codes that are mandatory for all Air Force information system programs. Application of the core codes to all future software developments will ensure proper integration with prescribed software architectures. Software applications so developed will support standard data elements and interface efficiently with key migration systems such as the projected common operating environment of the Global Command and Control System. In addition, compliance with the Air Force Technical Architecture will aid in the timely exploitation of new commercial products and services and facilitate software reuse.

Standard data elements are the fundamental interoperability-enabling feature of all information architectures. They are the basis for common interpretation, processing, and display of information, efficiency of communications, and interoperable, reliable, efficient software applications. Rigorous engineering techniques must be applied to consistently produce and transfer error-free data. The data standardization and data modeling policies and procedures will be compliant with and incorporated into the DoD Data Dictionary System. These activities are fundamental to implementation of the HORIZON vision.

C4I-00008

COMMAND AND CONTROL SYSTEM





Foreword

The Global Command and Control System (GCCS) will provide the warfighter a fused picture of the battlespace. It is an important cornerstone for the midterm phase of the Command, Control, Communications, Computers and Intelligence for the Warrior (C4IFTW) concept.

GCCS will have the capability of meeting warfighter needs well into the 21st century. It incorporates the core planning and assessment tools required for the combatant commanders and subordinate joint force commanders and it will meet the readiness support requirements of the Services. GCCS moves the warfighter's joint C2 support capability into the modern era of open systems architecture by migrating largely preexisting systems and mission applications to a common operating environment. The standards and unifying approach that GCCS has established are essential for DOD components to successfully reduce the large number of systems in use today.

I have witnessed GCCS in action during real-world crises and wholeheartedly support the system. GCCS provides the predominant source from which the warfighter generates, receives, shares, and utilizes information.

JOHN M. SHALIKASHVILI
Chairman
of the Joint Chiefs of Staff

All new ideas begin in a non-conforming mind that questions some tenet of the conventional wisdom.

H. G. Rickover

Vision

The Warrior needs a fused, real-time, true picture of the battlespace and the ability to order, respond and coordinate vertically and horizontally to the degree necessary to prosecute the mission in that battlespace.

Joint Pub 6-0

The Global Command and Control System (GCCS) is the mid-term implementation of the Command, Control, Computers, Communications and Intelligence for the Warrior (C4IFTW) concept, which fulfills the requirement for a capability to move a U.S. fighting force on the globe at anytime, and to provide it with the information and direction to complete its mission. C4IFTW is a revolutionary approach to address joint C4I interoperability issues and evolve heterogeneous Service C4I programs into a unified system.

GCCS is a key C4I system in satisfying the C4IFTW concept. It provides a fused picture of the battlespace within a modern C4 system capable of meeting warfighter needs into the 21st century. GCCS incorporates the core planning and assessment tools required by combatant commanders and their subordinate joint force commanders and meets the readiness support requirements of the Services. In moving the joint C2 support capability into the modern era of client/server architecture using commercial, open systems standards, GCCS brings to the ongoing DOD C4I migration strategy essential tools for the Services and agencies to successfully reduce the large number of systems in use today. GCCS is a user-focused program under the oversight of the Office of the Secretary of Defense ASD(C3I) and the Joint Staff.

Background

With the C4I for the Warrior Initiative led by the Joint Staff and supported by DISA, the Services are all looking at a common goal--achieving seamless C2 from the warfighting CINC to the tactical unit. GCCS is the method whereby this goal is to be achieved.

CINCUSACOM, March 1994

The World-Wide Military Command and Control System (WWMCCS), a mainframe system based on 1970's technology, has long been our "go to war" command and control system for force planning and deployment. During the 1980's a large-scale effort using classical acquisition strategies was undertaken to upgrade the existing environment with new technologies. The approach proved cumbersome, while warfighter needs were increasingly unfulfilled.

In September 1992 the Under Secretary of Defense (Acquisition), terminated the WWMCCS ADP Modernization (WAM) Program. He directed that "a new acquisition approach" be used to fulfill critical command and control mission needs. The Assistant Secretary of Defense (C3I) subsequently established the Global Command and Control System as the principle migration path for defense-wide command and control systems, directing that GCCS rapidly and efficiently deliver to combatant commanders C2 capabilities through maximum use of commercial off-the-shelf and government off-the-shelf components. Further, he specified that the program evolve through a continuous requirements refinement process to meet the goal of providing responsive C2 to combatant commanders.

GCCS has evolved from an initial baseline of existing C2 components. This baseline has served as the cornerstone for the rapid implementation of an initial system capable of fulfilling the most immediate user requirements and it will allow the shutdown of WWMCCS. As new GCCS versions are subsequently fielded, additional existing legacy systems will be replaced and secured. The common functional, physical, and operational characteristics of GCCS are based on a single Common Operating Environment. All future Joint and Service/CINC unique mission applications must be compatible with this COE. We will retain a fully integrated, single GCCS, with all applications having a common look and feel.

GCCS System Description

We are breaking new ground in establishing and benefitting from a truly worldwide, interoperable Global Command and Control System, with more capabilities and joint functionality to come.

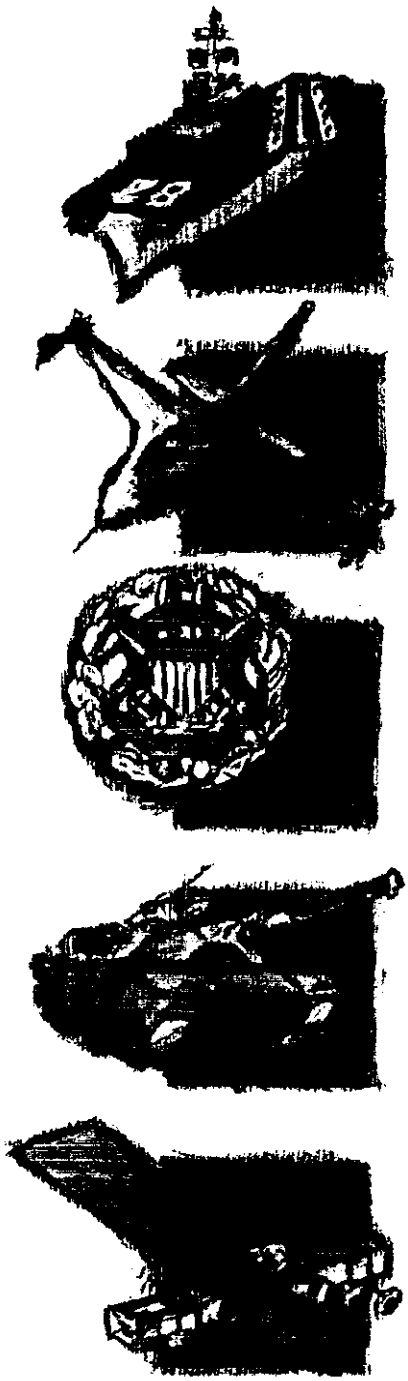
COMNAVCENTCOM
February 1995

GCCS is composed of several mission applications built to a single common operating environment networked to support sharing, displaying, and passing of information and databases. The GCCS infrastructure consists of a client server environment incorporating UNIX-based servers and client terminals as well as personal computer (PC) X-terminal workstations; operating on a standardized local area network (LAN). The GCCS infrastructure supports a communications capability providing data transfer facilities among workstations and servers. Connectivity between GCCS sites is provided by the Secret Internet Protocol Router Network (SIPRNET), the secret layer of the Defense Information Systems Network (DISN). Remote user access is also supported via dial-in communications servers, or via TELNET from remote SIPRNET nodes.

The baseline GCCS architecture consists of a suite of relational database and application servers. At most GCCS sites, the relational database server acts as a typical file server by hosting user accounts, user specific data, and site specific files not part of GCCS. The application servers host the automated message handling system, applications not loaded on the database server and other databases.

At each GCCS site, one application server is configured as the executive manager (EM) providing LAN desktop services. It also hosts applications not loaded on the database server. The EM server acts as the user interface providing access to GCCS applications through user identification and discrete passwords. GCCS software applications are categorized into two groups: Common Operating Environment (COE), and Mission applications.

The Common Operating Environment



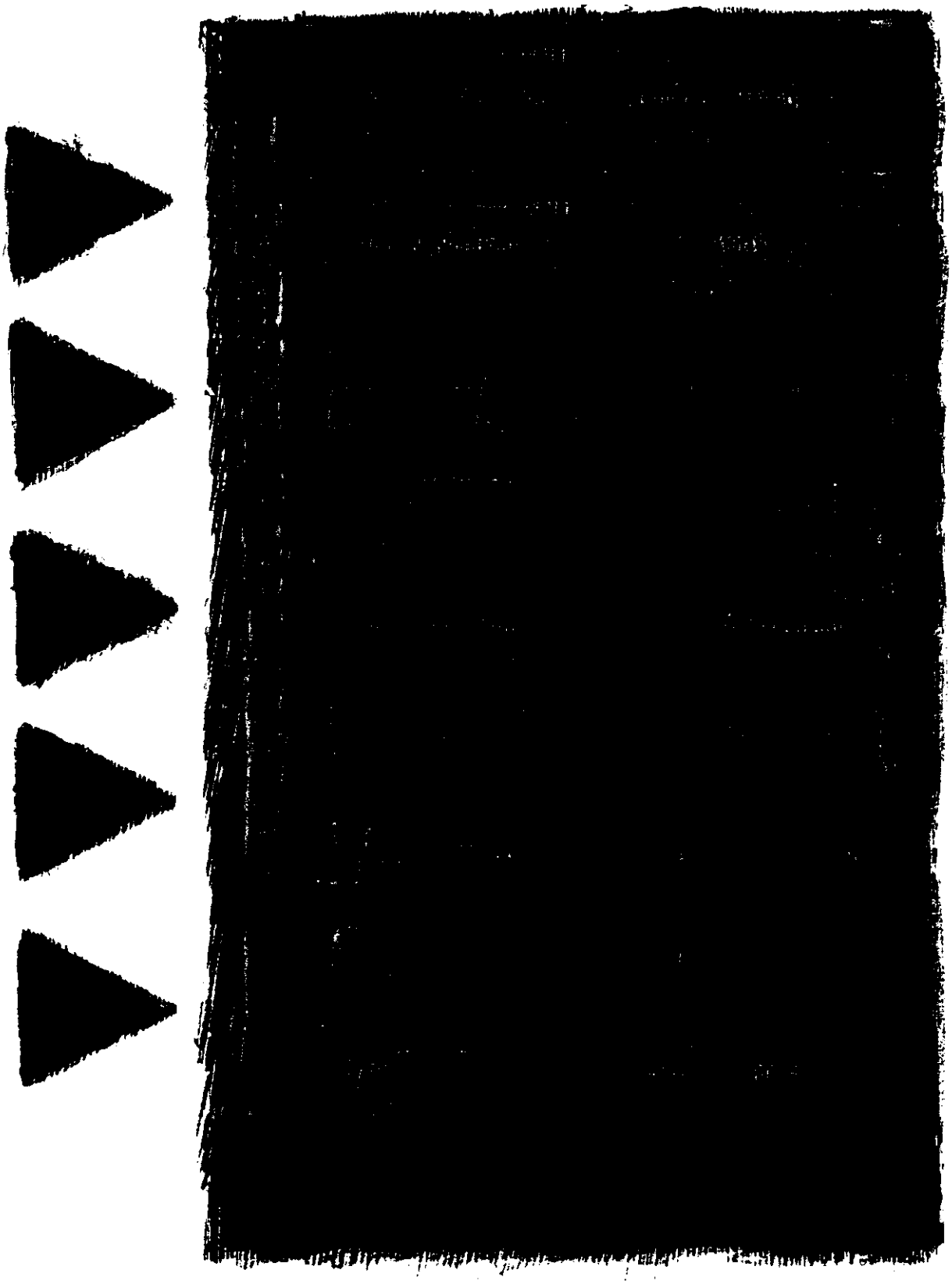
The Defense Information Infrastructure (DII) Common Operating Environment (COE) provides a standard environment, "off-the-shelf" software, and a set of programming standards that describe in detail how mission applications will operate in the environment. The COE contains common support applications and platform services required by mission applications. Each application that is migrated to the common environment must comply with published guidance described in the Integration and Runtime Specification.

Does the COE provide everything to all mission applications today? Not yet, but it will. Currently, workarounds are created as mission applications migrate to the COE, but these work-arounds are being kept to a minimum. As the COE matures, the workarounds will no longer be needed, and they can be quickly and easily "stripped" from the mission applications.

How will the COE work for the user? As the user selects mission applications needed to complete an assigned mission, the integration tool automatically loads all the COE modules those applications will use. These selected modules make up a subset of the DII COE superset; this subset is called a COE-variant (COE-V). The original COE software components are used without modification. System managers must ensure that COE-V's do not include non-standard software that duplicates functions provided by software under the COE.

MISSION APPLICATIONS

Objective COE



...Using Standard Data

The evolutionary approach integrating our existing software is right. We must continue to push forward with our migration efforts while ensuring that the users' requirements are met.

DEPSECDEF, August 1994

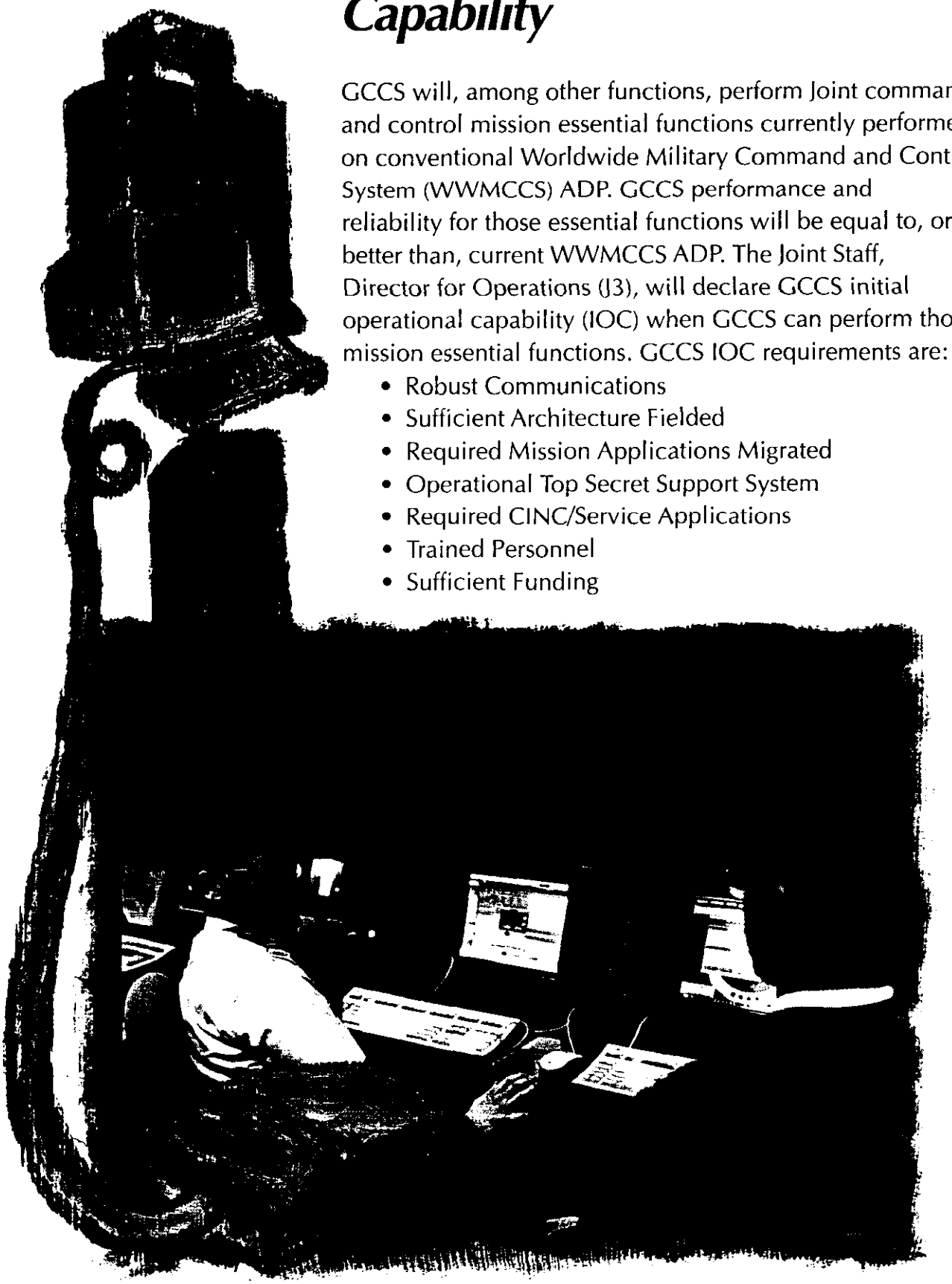
The use of standard data elements is key to any automated system success's, especially command and control systems. Using standard data eliminates redundancies and provides a common base to facilitate information exchange, reducing time needed to set up a basis for data communication.

One of the results of stovepipe systems within the DOD was the proliferation of non-homogeneous databases. Although each system worked adequately within the particular component for which it was built, there was no interoperability with other components. Yet each component had information that needed to be shared with other components. The best solution to this untenable situation is the use of standard data. The question was where to start.

The Services, combatant commands, and agencies answered that question by declaring that GCCS must, at a minimum, provide the same operational planning functionality that the WWMCCS provided via the Joint Operation Planning and Execution System (JOPES). The JOPES data model encompassed data requirements for many of the applications that would be included within GCCS. Clearly, the JOPES data model was the place to start standardizing data.

The Defense Information Systems Agency (DISA), acting for the Joint Staff, quickly developed a plan to approve over 1200 data standards defined in the JOPES data model. The data standards were divided into 9 logical packages and placed in directories as candidates for standardization. Data administrators from pertinent functional areas analyzed the data for usability, recommended modifications where needed, and finally declared the data as meeting approved standards. Future modifications and enhancements to GCCS and the other DOD functional area databases will use these approved standards. The DOD had taken an important step in information exchange.

GCCS Initial Operating Capability



GCCS will, among other functions, perform Joint command and control mission essential functions currently performed on conventional Worldwide Military Command and Control System (WWMCCS) ADP. GCCS performance and reliability for those essential functions will be equal to, or better than, current WWMCCS ADP. The Joint Staff, Director for Operations (J3), will declare GCCS initial operational capability (IOC) when GCCS can perform those mission essential functions. GCCS IOC requirements are:

- Robust Communications
- Sufficient Architecture Fielded
- Required Mission Applications Migrated
- Operational Top Secret Support System
- Required CINC/Service Applications
- Trained Personnel
- Sufficient Funding

Testing—A Continuous Process

As GCCS starts the assessment period and proceeds toward initial operating capability, it is appropriate to reflect on how far we have come with fulfilling the C4I for the Warrior vision.

CINCUSACOM, September 1995

GCCS testing is based on a process of continuously evaluating the comprehensive system. DISA, the operational users, and DOD Operational Test and Evaluation (DOT&E) will each evaluate GCCS to ensure its continued operational effectiveness and suitability. The testing process continues to track the progress of GCCS throughout its integration and installation phases. It occurs concurrently as additional functional blocks are added to the system. The process provides a complete, accurate, and timely evaluation of the system. The results from the testing support GCCS in three areas:

Providing input on systems or software nominated for the "Best of Breed" selection process

Providing information on how well a candidate system operates in the GCCS environment, supporting system integration decisions

Providing feedback to determine satisfaction of user requirements and facilitate changes to GCCS

The testing process verifies that GCCS meets the stated requirements of the users, from the National Command Authority to Joint Task Force commanders. It ensures that GCCS remains interoperable and fully integrated.

"Best of Breed"

Mission application software nominated by a Service, combatant command, agency, or other DOD entity for inclusion in GCCS is known as candidate "Best of Breed" software. Candidates are submitted to functional working groups or to the System Integration Working Group (SIWG) for analysis.

The functional working groups identify and prioritize user requirements, then solicit nominations of existing applications from the Services, combatant commands, and agencies to satisfy the requirements. The working groups evaluate the nominated applications, both functionally and technically, before recommending an application to the GCC Review Board. The General/Flag Officers Advisory Board gives final approval to "Best of Breed" nominations.

The nominating organization of a selected "Best of Breed" application will usually remain the executive agent for that application, ensuring continuing support and technical expertise for users of the application.

Training the Trainer

GCCS enabled USTRANSCOM to more effectively support the Chairman's accelerated planning cycle.

USTRANSCOM J3/J4/J6, June 1995

Rapid, responsive and quality training for GCCS users has been the challenge and cornerstone to successful implementation of GCCS. And the United States Air Force's Air Education and Training Command (AETC) and Joint Operation Planning and Execution System (JOPES) Training Organization (JTO) have risen to that challenge.
An 8 August 1994 Memorandum of Agreement between the Joint Staff and Headquarters, United States Air Force, designated the Air Force as the GCCS single service training manager (SSTM).

The SSTM, located at Keesler Air Force Base, Mississippi, manages resources for GCCS technical training, including system, network, database administration, operating systems, and user training operations. Fixed classroom sites, mobile training teams, and documentation are available. Likewise, JTO, located at Scott Air Force Base, Illinois, manages resources for all JOPES-related training through fixed classroom sites and mobile training teams.

Technical and JOPES-related training activities are coordinated through the SSTM and JTO, respectively, both of which are supported by military, DOD civilian and contractor trainers. Using a "train the trainer" approach, a cadre of personnel from each GCCS site receive formal training and then return to their sites around the globe to train additional personnel. This approach ensures an efficient, timely distribution of GCCS knowledge in harmony with rapid, nimble GCCS integration efforts.

Scheduling and Movement (S&M) handles command and control information on deployment activity and status. It functions as a vehicle for the scheduling and tracking movement of TPFDD requirements.

Logistics Sustainment Analysis and Feasibility Estimator (LOGSAFE) assists logistics planners in determining sustained movement requirements during deliberate and crisis action planning.

Joint Flow and Analysis System for Transportation (JFAST) is an analysis tool which provides users the ability to determine transportation feasibility of an Operation Plan (OPLAN) or Course of Action (COA).

Joint Engineer Planning and Execution System (JEPES) provides planners with a method to determine requirements and/or adequacy of engineering support provided in OPLANs or COAs.

Medical Planning and Execution System (MEPES) provides contingency medical support information for allocating medical resources.

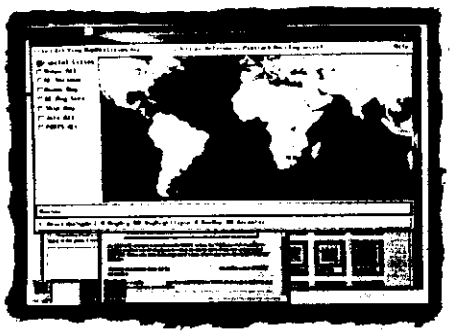
Non Unit Personnel Generator (NPG) functions are to assist in determining quantities of replacement and filler personnel.

Ad Hoc Query (AHQ) provides users with a means to develop, save, and print tailored queries extracting data from the JOPES core database.

Systems Support functions as the JOPES core database management subsystem for functional managers.

Airfields is an information retrieval application providing the user with the capability to access, extract, and print information from the Automated Air Facilities Information File database.

Global Reconnaissance Information System (GRIS)



GRIS supports the planning and scheduling of monthly sensitive reconnaissance operations (SRO) theater requests. The Joint Staff staffs these requests through the office of the Secretary of Defense, Central Intelligence Agency, and State Department for National Security Council approval. Incoming RECON 1/2/3/4 formatted messages are received by an automated message handling system, validated, and passed to the GRIS application for automated processing and database update. GRIS generates all RECON messages and also monitors the monthly execution of theater reconnaissance missions approved in the previous month. GRIS is used by the Joint Staff and theater commands exercising operational control (OPCON) over airborne reconnaissance assets.

Evacuation System (EVAC)

EVAC collects and displays information about US citizens located outside the United States as collected by US State Department embassies and consulates. It accesses the database server via TELNET operation from a GCCS compatible client.

Fuel Resources Analysis System (FRAS)

FRAS provides fuel planners an automated capability for determining supportability of a deliberate or crisis action plan and for generating the time-phased bulk petroleum, oil and lubricants required to support an OPLAN. FRAS facilitates review of the fuel requirements of a proposed, new, or revised OPLAN and assesses adequacy of available resources to support crisis action planning. Requirements can be generated and analysis performed for the overall OPLAN, regions within the OPLAN, by Service, and within Service by regions. Two or more OPLANs can

be combined into a single OPLAN for analysis. The requirements generated can be varied through the use of intensity tables and consumption data extracted from the Logistics Factors File (LFF) or with Service-provided data system.

Global Status of Resources and Training (GSORTS)

GSORTS provides information on status of units with respect to personnel, equipment and training. Query and display capabilities include: categories of units (ships, fighter aircraft, ground forces, etc.); specific types of units (frigates, armor battalions, F-15's, etc.); and by specific unit (displays detailed status information).

Joint Maritime Command Information System (JMCIS)

JMCIS is the foundation for the GCCS fused operational battlespace picture. It provides near real-time sea and air tracks. JMCIS receives inputs from different systems, and can interface with other systems. JMCIS uses a core service, known as unified build, to provide geographic display, contact correlation, and track data base management.

Theater Analysis and Replanning Graphical Execution Toolkit (TARGET)

TARGET contains a set of planning tools designed to support the operational planner during crisis action procedures. These tools allow planners and operators to accomplish tasks through rapid access to required documents, information sources, analysis tools, multi-media and teleconferencing tools.

Joint Deployable Intelligence Support System (JDISS)

JDISS applications provide the intelligence window to access national, theater, and tactical intelligence sources through the joint architecture for intelligence. It provides connectivity and interoperability with intelligence systems required to support forces during peacetime, crisis, and war. JDISS includes INTELINK at the Secret classificatiion level (INTELINK-S). It is an intelligence dissemination service which enhances the sharing of intelligence information electronically over the SIPRNET. INTELINK provides intelligence dissemination using networked information discovery, retrieval, and browsing services. Its "point and click" technology makes intelligence products widely available to both users and producers of intelligence.

Air Tasking Order (ATO)

ATO provides the capability to view and print selected portions of air tasking orders. A query function allows the user to tailor requests for information contained in a specified order for viewing. The query function also supports display of color-coded ground tracks for selected portions of the order. ATO interfaces with the Contingency Theater Automated Planning System (CTAPS).

Conclusion

The Global Command and Control System is bringing the C4I for the Warrior vision into reality and the promise to provide warfighters with a fused, real-time picture of the battlespace. Ultimately, GCCS will provide command and control of our forces across the full range of military operations and through each phase of force projection.

GCCS gives the warfighter a highly flexible system capable of collecting, processing, disseminating and protecting information to support critical decision-making and to achieve unity of effort and command dominance.

Interoperability has been the driving force in implementing GCCS. Common mission applications, databases, imagery, teleconferencing and open architecture are key tenets in providing a single joint Command and Control system. The system has been designed to grow to meet the needs of the warfighter of the future and the challenges of multiple regional conflicts.

Office of Primary Responsibility: Joint Staff
J6V, Washington D.C. 20318-6000,
Commercial: (703) 614-5908,
DSN: 224-5908, FAX: (703) 697-4937,
DSN: 227-4937,
Internet: mForbes @ ls1.JS.mij

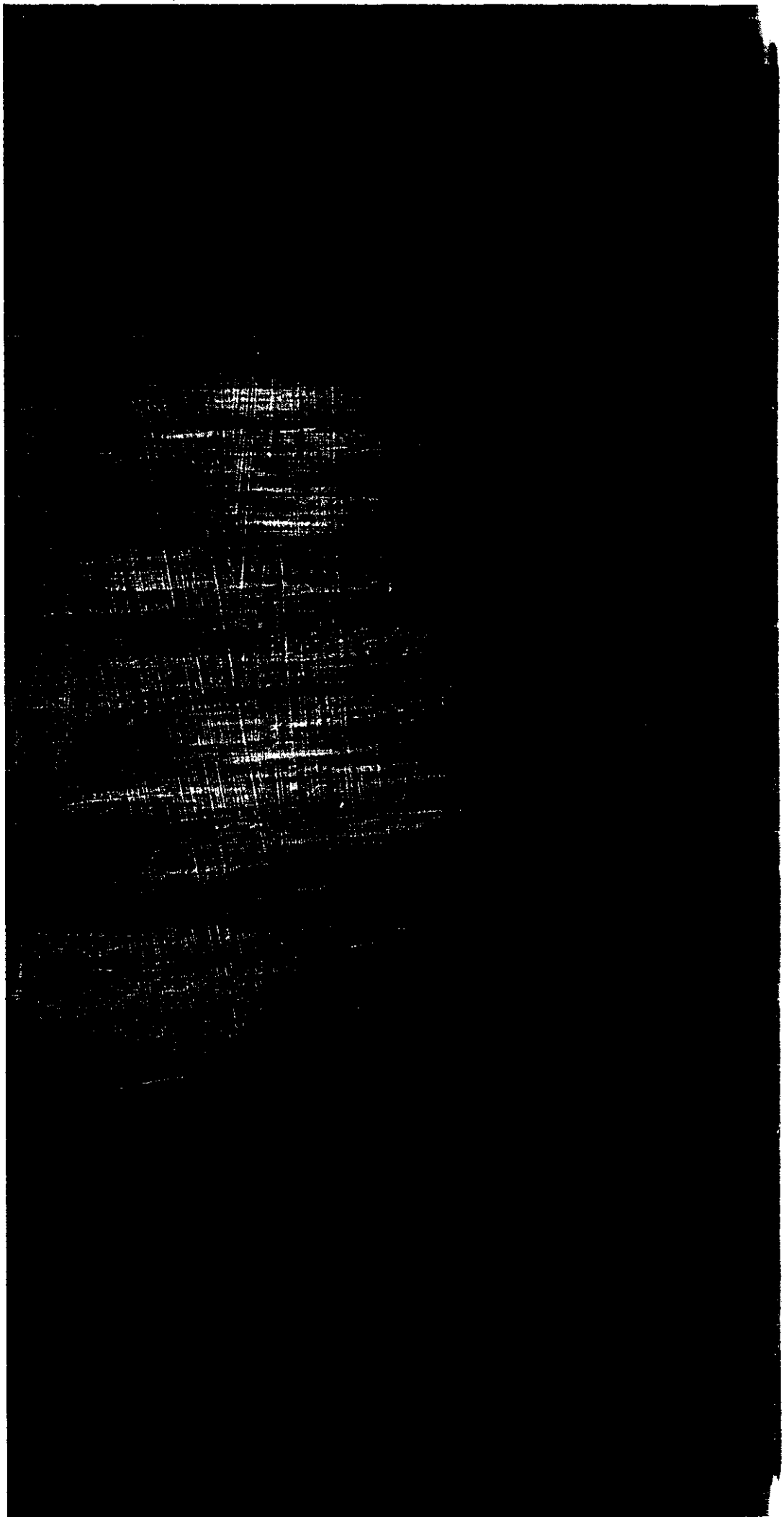
Photographs: *Mr. Cecil Webb,* 11th Wing, Media Services, Pentagon.

Department of Defense Joint Combat Camera Center, First Combat Camera Squadron, Det 9.

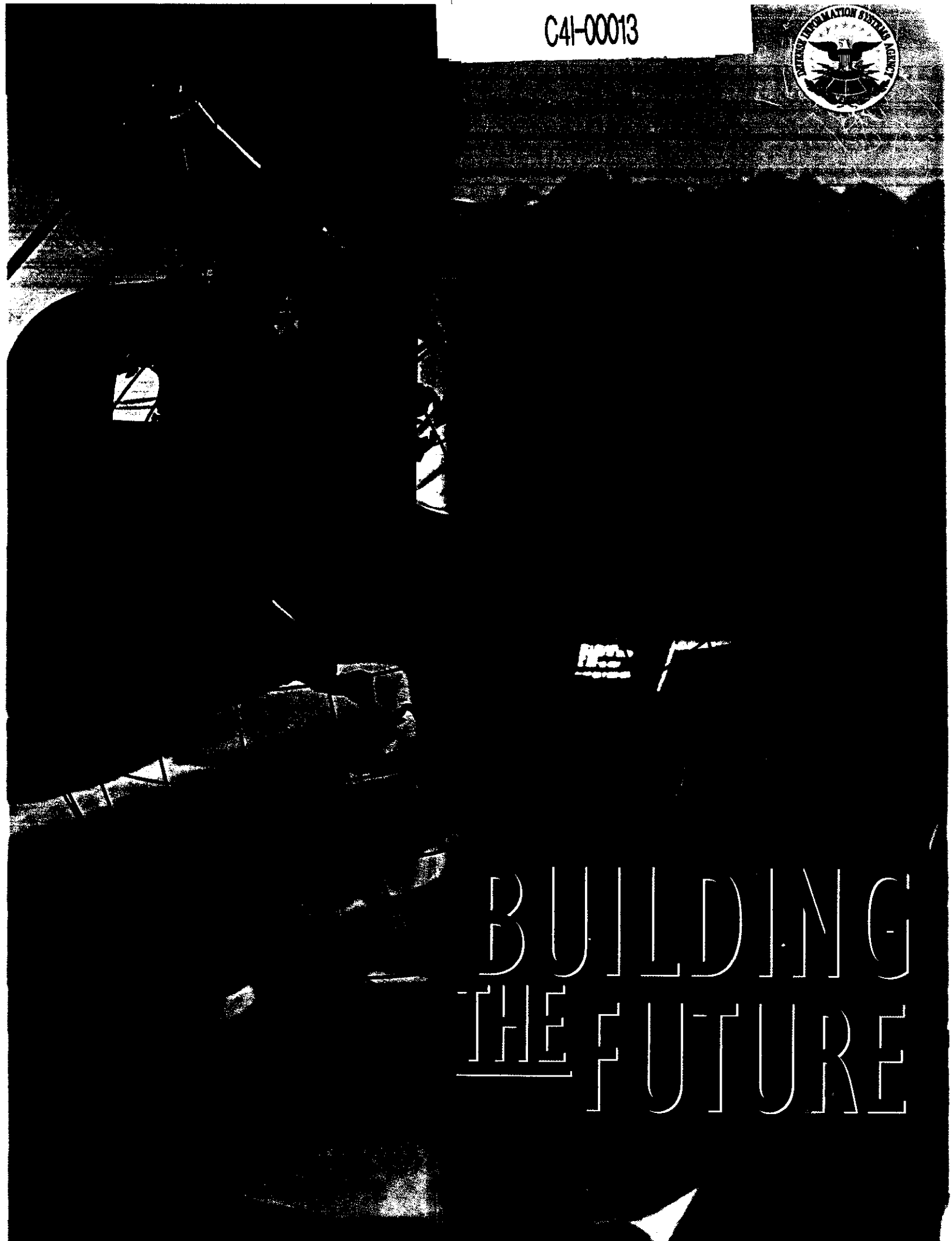
Art Direction: *Ms. Mary Walden,* 11th Wing, Media Services, Pentagon.

Computer Graphics: *SSgt Patrick B. Morrow,* 11th Wing, Media Services, Pentagon.

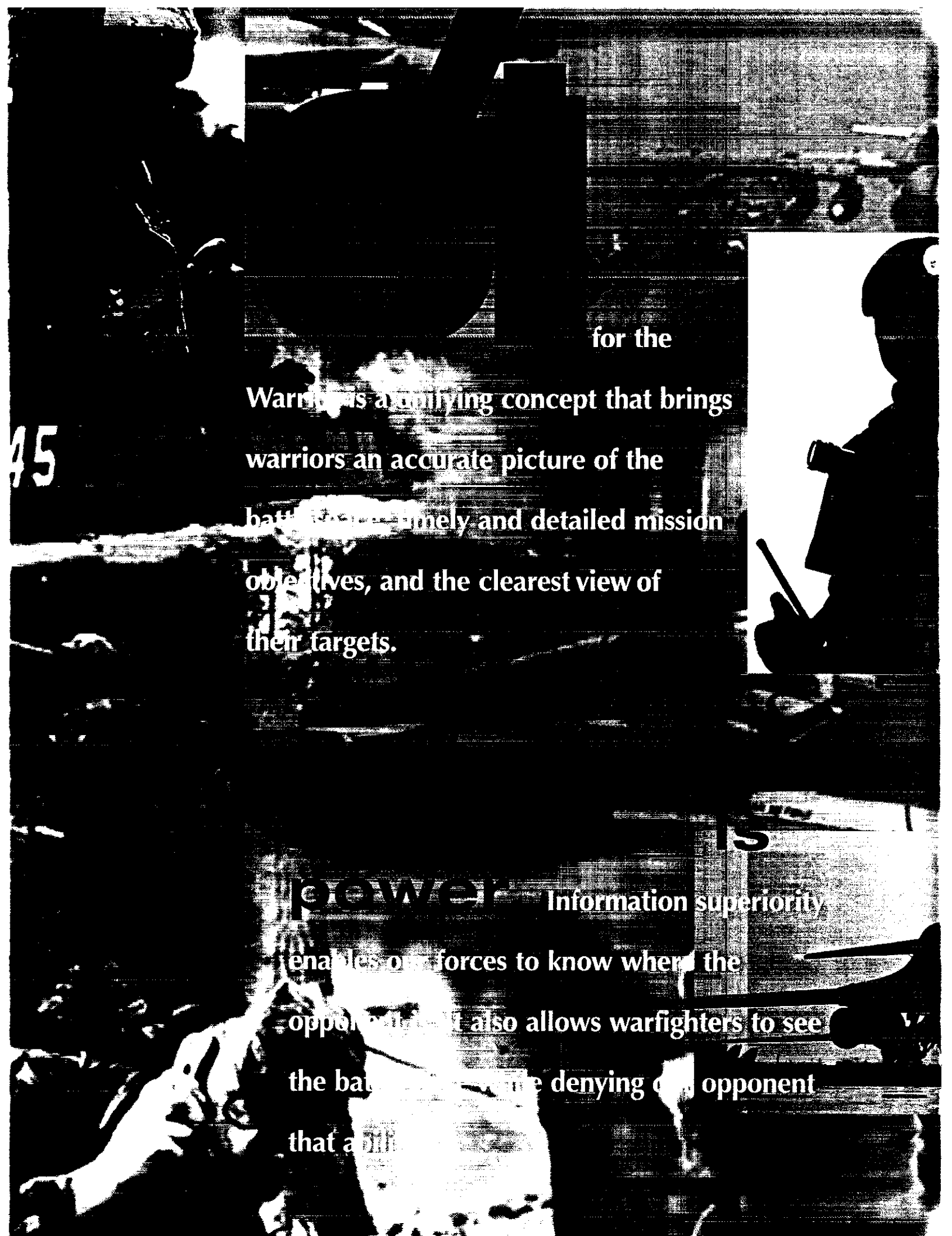
Origional Cover Art: *Mr. Nilo Santiago,* 11th Wing, Media Services, Pentagon.



C41-00013



BUILDING THE FUTURE



for the Warrior is a unifying concept that brings warriors an accurate picture of the battlespace, timely and detailed mission objectives, and the clearest view of their targets.

Information superiority enables our forces to know where the opponent is. It also allows warfighters to see the battlespace while denying our opponent that ability.

Information Systems Security (INFOSEC)

Summary

INFOSEC is the measures and controls that safeguard and protect an information system from unauthorized disclosure, modification or destruction from such threats as hackers, terrorists and foreign governments. The Defense Information Systems Agency, (DISA) as central manager of the Defense Information Infrastructure (DII) and in joint cooperation with the National Security Agency (NSA), defines INFOSEC requirements and implementation into the DII. The Defense Intelligence Agency (DIA) supports these activities with threat assessments.

Facts/Discussion

The DII is a seamless web of communications networks, computers, software databases, applications, facilities and other capabilities that meet the Department of Defense's (DOD) information processing and communications needs. Information systems cannot be protected with a single mechanism. DISA must ensure that the DII contains the adequate protection against attack by using a layered defense.

Under the Multilevel Information Systems Security Initiative (MISSI), NSA is developing a complete suite of security products which include the FORTEZZA family of crypto cards, firewalls and multilevel security guards/gateways which DISA is implementing to protect the DII. DISA is working to ensure that information security is integrated into all of its programs from the beginning.

The Global Operations and Security Center (GOSC) consolidates the functions of the Global Control Center and the Automated Systems Security Incident Support Teams (ASSIST) into one organization. This consolidates all aspects of security into the day-to-day management and operation of the networks supporting the Department of Defense. The center monitors, detects, and reacts to disruptions in the infrastructure. The center also includes daily operation of the Vulnerability Analysis and Assessment program (VAAP). This program provides an evaluation of the overall security posture of the DII by way of intrusion penetration testing. The Defense Intrusion Analysis and Monitoring Desk (DIAMOND) is located in the center and provides advanced analysis of intrusion data and network sensors looking for unauthorized activity. The GOSC also provides DOD-wide support for the detection, analysis and removal of malicious code (more commonly known as viruses, logic bombs, etc.).

The INFOSEC Program Management Office (IPMO) consolidates the acquisition, implementation, integration and dissemination of INFOSEC products and services into the DISA pillar programs (e.g., DISN, DMS, GCCS, and GCSS) and other DOD systems and activities. The IPMO coordinates with the CINCs, Services and Federal Agencies to determine requirements and develop standardized INFOSEC tools, methods, and training and awareness products, which help to ensure the confidentiality, integrity and availability of warfighter information systems. The IPMO provides INFOSEC technical support functions to include INFOSEC certification, connection approval and compliance validation of connections to the DII. The IPMO also manages development and fielding of standard multilevel security capabilities supporting CINC, Service and Agency C4I requirements.

DISA supports Information Warfare - Defense activities of intelligence organizations, the CINCs Services, other Federal Agencies, and the private sector.

(As of February 1997)

Global Combat Support System (GCSS)

Summary

The C4I for the Warrior (C4IFTW) concept is committed to meet the warrior's information requirement to achieve victory for any mission, at any time, and at any place. C4IFTW is the vision and roadmap for creating an integrated combat support picture for the warfighter.

GCSS is the final piece of the C4IFTW concept. It is a demand-driven, joint warfighter-focused initiative to accelerate delivery of improved combat support capabilities. Using the same approach, methodology, practices, tools, and integration procedures as the Global Command and Control System (GCCS), GCSS is an initiative that integrates existing combat support systems to gain efficiency and interoperability in support of the warfighter. GCSS will provide the warfighter with a fused, real-time combat support view of the battlespace.

Facts/Discussion

Currently, the Joint Task Force has stovepiped information systems in logistics, personnel, engineering, finance, acquisition, and health services. GCSS will eliminate these stovepipe systems and develop a shared information database access via a single computer.

One of the components of GCSS is the Electronic Commerce (EC)/Electronic Data Interchange (EDI) infrastructure initiative. This initiative enables the warfighter to electronically access goods and services in a timely and efficient manner via the Electronic Commerce Infrastructure (ECI).

GCSS will create a technical environment and process to economically integrate existing computer-based systems software and hardware using the common operating environment (COE) and shared data environment (SHADE). It will also expand the GCCS COE to accommodate combat support applications and will also provide "split base-reachback" capabilities from the foxhole to the sustaining base to allow the warfighter to be "deployed" by electronic means.

GCSS provides on-line connectivity to NIPRNET/SIPRNET web and access to applications and data. GCSS will have heavy user participation, and through incremental improvement will evolve to hardware independence and interoperability.

GCSS goals are to:

--Provide the warfighter reachback to combat support capabilities and personnel that remain in garrison.
--Provide a combat support infrastructure that is responsive to joint mission support needs.
--Provide a flexible and adaptive open computing environment.
--Enable interoperability and integration across combat support areas and from combat support to the combat environments.
--Integrate and implement an information infrastructure that provides end-to-end information connectivity and access.

GCCS and GCSS both need the Defense Information System Network (DISN) and the Defense Message System (DMS) to complete C4IFTW. GCSS will rely on all components of the DISN for information transport services including voice, text, and imagery. DMS provides the warfighter a secure, reliable, and accountable writer-to-reader messaging infrastructure at reduced cost.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of June 1997)

Global Command and Control System (GCCS)

Summary

The C4I for the Warrior (C4IFTW) concept is committed to the challenge of meeting the warrior's quest for information needed to achieve victory for any mission, at any time, and at any place. C4IFTW is the vision and roadmap for creating a broadly connected joint system providing total battlespace information to the warrior.

Joint operations involving multiple land, sea and air units in adaptive joint force structures increasingly require joint networks and joint systems that are fully interoperable horizontally across air, sea, space and ground environments. This is the ultimate goal of C4IFTW. The Global Command and Control System (GCCS) is the midterm solution and the bridge to the concepts outlined in the C4IFTW concept. GCCS is C4IFTW in action, today.

Facts/Discussion

GCCS is a common operating environment (COE), integration standard, and migration strategy that eliminates the need for inflexible stovepipe command and control systems and expensive duplication. It is the migration of existing systems into a new COE connected across the Secret Internet Protocol Router Network (SIPRNET) and the integration of selected command and control (C2) systems into a comprehensive, interoperable system.

Its first priority is to demonstrate the C4IFTW concept's vision by becoming a globally connected, warrior-involved, interoperable, fully-integrated C4 system. The GCCS core consists of the basic functions required by the warfighter to plan, execute, and manage military operations. These functions are then satisfied by selecting the applications from existing C2 systems that best meet the requirement. This ensures interoperability, minimizes training requirements and allows efficient use of limited defense resources. GCCS has been identified by the Assistant Secretary of Defense for Command, Control, Communications and Intelligence as the C2 migration system to meet the goal of migrating the many Service systems into fewer, better integrated systems.

GCCS is not a traditional acquisition program nor a grand design effort that is difficult or cumbersome. It remains simple and straightforward, being implemented one step at a time as user feedback helps build the next step. It implements a flexible and highly adaptive client-user architecture, tailored for the warfighter as specified by the warfighter.

On August 30, 1996, DISA officially pulled the plug on the Worldwide Military Command and Control System (WWMCCS) Intercomputer Network (WIN). Concurrently, the Joint Staff declared the Global Command and Control System (GCCS) as the joint command and control system of record.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of June 1997)

Defense Message System (DMS)

Summary

DMS consists of all the hardware, software, procedures, standards, facilities and personnel needed to exchange electronic messages among organizations and individuals in the Department of Defense (DOD) whether at home base, while traveling or when deployed. DMS will provide a common messaging environment that is flexible and interoperable between the Military Services, Agencies, Joint Staff, Federal Agencies, our Allies, and the public.

Using the global Defense Information System Network (DISN) transmission system and supporting local/tactical infrastructure capabilities, DMS provides electronic messaging, directory, security, and management services for DOD organizations and individuals.

Goals and Development

For the past 35 years, AUTODIN has provided DOD with unprecedented messaging support. Although the system has undergone numerous enhancements, its basic framework is 1960's proprietary technology; consequently, it cannot be easily upgraded to support today's information requirements.

When the DMS program began, it established two keys goals: 1) develop a system that reduced the high operation and maintenance costs associated with AUTODIN, and 2) improve messaging support to the warfighters.

To achieve these and other goals, the DMS program turned to commercial industry for solutions. Rather than build another proprietary system with enhanced capabilities (in essence, a new and improved AUTODIN) the program sought commercial product offerings to meet the full range of DOD's needs. The program first established a baseline from which proposed DMS costs and benefits could be measured. Using validated requirements and established commercial technology objectives, a DMS target architecture was defined with an accompanying implementation strategy to evolve from the baseline to the target.

Acquiring the System

In January 1993, the Defense Information Systems Agency (DISA) was tasked to lead the continued development of an integrated system that provided advanced messaging and directory services, and phase out the AUTODIN system. The DMS "continuous evolution" approach has kept the program in step with commercial industry trends.

The DMS program employs an innovative acquisition strategy designed to influence development of mainline commercial products while maintaining maximum competition and acquisition flexibility. Through this acquisition, vendors are encouraged to provide commercial

product solutions to meet DOD messaging and directory service needs. These solutions, which require the incorporation of international standards, ensure essential characteristics that include connectivity, interoperability, accountability, reliability and security. In keeping with common commercial practice, major commercial vendors provide these features as "add-ins" to their core commercial offerings.

Track I of the dual-track DMS acquisition is designed to acquire the baseline DMS secure, accountable, and reliable "system" consisting of the managed global infrastructure and initial DMS compliant user components. Execution of Track I began when DOD awarded an Indefinite Delivery, Indefinite Quantity (IDIQ) acquisition contract for DMS-compliant products and services to Lockheed Martin Federal Systems (LMFS) in May 1995.

An independent compliance test and evaluation program, administered by the DISA Joint Interoperability and Test Command (JITC), has been developed to test and certify Track I products from the LMFS contract as well as Track II products from other vendors.

DMS Today

On 3 June 1997, 13 Track I products from the LMFS contract completed DMS compliance Test and Evaluation (CT&E) and were posted to the DMS Certified Compliant Products List (CCPL). These products, comprising the baseline DMS "system," serve as "reference implementations" of DMS compliant products as Track II products enter the compliance test and evaluation process. Track I compliant products are from CommPower, Enterprise Solutions, Ltd, LMFS, Lotus Development, Microsoft, and Xerox. Novell is the first Track II vendor to enter the CT&E process and more than 20 additional vendors have expressed interest in submitting their products for DMS compliance testing.

Initial Operational Test and Evaluation (IOT&E) of the initial DMS system (Release 1.0) commenced on 28 May 1997 and will continue through July. As this basic DMS capability completes operational testing, the next DMS release (1.1) is under development and scheduled to enter streamlined compliance testing in September 1997. As operational experience is gained, problems will be resolved and additional functionality added through additional DMS releases approximately every 6 months. Concurrent testing of each new release and development of the following release is a necessary aspect of maintaining currency with commercial technology.

Simultaneously, the Joint DMS Community is defining flexible DMS implementations that allow DOD users and organizations to take full advantage of features such as collaborative computing that DMS compliant commercial products offer in conjunction with their messaging features. The ultimate DMS objective is to remain firmly within the commercial technology mainstream while ensuring satisfaction of validated DMS requirements.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of June 1997)

Defense Information System Network (DISN)

Summary

The Defense Information System Network (DISN) comprises the DOD consolidated worldwide enterprise-level telecommunications infrastructure which provides the end-to-end information transport for supporting military operations, national defense C3I requirements, and corporate defense requirements. DISN provides the primary transmission path to support the Defense Information Infrastructure (DII). DISN features a backbone capability in CONUS with Synchronous Optical Network (SONET) transmission. This transmission is integrated with military and commercial leased communication satellites, switched voice and data services, SONET bandwidth managers, and teleconferencing services.

Facts/Discussion

In July 1995, DISA announced its strategy for the next generation global telecommunications infrastructure that would support the Nation's Warfighters worldwide. As a result, DISN would replace expiring contracts and aging systems with a global approach designed to take maximum advantage of industry capabilities and evolving technologies. The goal architecture represented a graceful technological evolution from the use of DOD-owned and operated networks and systems to commodity services where possible.

The DISN strategy will consolidate more than 100 independent DOD networks into a single, integrated, cost effective, efficient, common-user global "infosphere," a grid that will provide connectivity on demand anytime, anywhere. This will help alleviate the problem with individual legacy communications systems which are not effectively integrated and often non-interoperable. Today, these disparate systems impede or even prevent the exchange of information between warfighting commands and units. DISN serves as the evolving DOD worldwide protected network allowing Warfighters to "plug in" and "push or pull" information in a seamless, interoperable and global battlespace.

DISN is a dynamic network, with the capability to accommodate emerging new or improved technologies that better serve the unique communication needs of the Warfighter. DISN provides seamless and interoperable information transport across strategic and tactical networks supporting Joint Task Forces and Combined Task Forces, as well as the telecommunications networks of non-defense agencies.

DISN will provide the transmission and switching of voice, data, video, and point-to-point bandwidth services for wide area, local area, metropolitan area, and long-haul networks.

DISN will use available commercial products and services, while providing DOD with the degree of network control necessary to ensure rapid response to the Warfighters. DISN integrated voice/imagery and data information transport will be transparent to the Warfighters, facilitate the management of information resources and be responsive to national security and defense needs under all conditions in the most efficient manner.

In early 1995, the Joint Chiefs of Staff (JCS) validated a Mission Need Statement (MNS) which realigns priorities from simple business-case services to a more secure and government controlled network of commercial switching nodes and leased transmission services. This focuses C4I more directly for the Warfighter.

In early 1996, the JCS issued a Capstone Requirements Document which clearly segments DISN into three distinct blocks. These blocks are base level, long-haul, and deployed. All blocks are to be implemented as fully interoperable blocks, but by different organizations, with the technical oversight of DISA. The Services will implement DISN on their respective bases, DISA will implement the long-haul block, and different Services or Agencies will be designated to jointly implement the deployed block.

Since July 1995 when the strategy was announced, DISA has awarded all four initial DISN contracts. The first contract, DISN Support Services - Global (DSS-G) contract, was awarded to Boeing Information Services, Inc. The DSS-G serves as the network's technical management support vehicle. The second contract, DISN Switched/Bandwidth Manager Services (DS/BMS-C), was awarded to MCI Telecommunications Corp and covers the continental United States (CONUS). In addition to supporting the vast majority of CONUS, this contract covers overseas traffic that originates or terminates in the 48 contiguous states.

The third contract, DISN Transmission Services - CONUS (DTS-C), was awarded to AT&T Government Markets. This contract will provide backbone and access area transmission services at T-1 and above bandwidth rates. The fourth contract, DISN Video Services - Global (DVS-G), was also awarded to AT&T Government Markets. AT&T will provide multi-vendor interoperability and dedicated video services including secure and non-secure, point-to-point and multi-point bridging, a reservation/scheduling system, video services management and monitoring, and provisioning and user-site network interface equipment.

DISA has also awarded the DISN Hawaii Information Transfer System (HITS) contract to AT&T Government Markets. This provides wide-area and local networking services to DOD facilities within the State of Hawaii.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of June 1997)

Defense Information Infrastructure (DII)

Summary

The DII is the web of communication networks, computers, software, databases, applications, weapon systems interfaces, data, security services, and other services that meet the information processing and transport needs of DOD users across the range of military operations. It implements the C4I For The Warrior (C4IFTW) vision of an user-driven infrastructure through which warfighters and other DOD users can quickly share needed information from any location, at any time using secure voice, text, and video services. The DII will allow warfighters to maintain information superiority by presenting a fused, real-time, true representation of the three dimensional battlespace.

Facts/Discussion

The DII will allow U.S. Forces to meet the needs of the National Military Strategy: U.S. Forces must be able to project power from Continental U.S. bases, sanctuaries and in-theater locations in times of conflict, plus support up-to-the-minute peacetime missions.

The DII will operate as a collection of distributed, heterogeneous information systems. It will range from DOD applications implemented at central locations, to base-level or end-user applications on desktops or in tactical environments. The infrastructure requires collaborative development reflective of its cooperative ownership among the Office of the Secretary of Defense (OSD), the Joint Staff and individual services and agencies.

The current DII consists of many elements, much like a puzzle in which each piece is crucial to the overall picture. These elements build on and include a foundation of integration and technology support. It is important that the DII evolve to support new and existing missions, to provide new capabilities, and to introduce new technology.

The DII encompasses:
--sustaining base, tactical, DOD-wide information systems. and Command, Control, Communications, Computer,m and Intelligence (C4I) interfaces to weapons systems
--the physical facilities used to collect, distribute, store, process, and display voice, data, and imagery
--the applications and data engineering practices (tools, methods, and processes) to

build and maintain the software that allow C2, intelligence, surveillance, reconnaissance, and mission support users to access, manipulate, organize, and digest proliferating quantities of information.
--the standards and protocols that facilitate interconnection and interoperation among networks and systems and provide security for the information carried.
--the people and assets which provide the integrating design, management and operation of the DII, develop the applications and services, construct the facilities, and train others in DII capabilities and use.

The Defense Information Systems Agency (DISA) works with the CINCs, Services and other Agencies to develop the DII Master Plan for ASD(C3I). The DII Master Plan is a living document that establishes the common DOD vision for the DII, identifies current and future elements, defines DII participants' roles, responsibilities and relationships, and identifies the relationships and interdependencies of key initiatives.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of June 1997)

The Defense Information Systems Agency (DISA)

The Defense Information Systems Agency (DISA) is a Department of Defense (DOD) combat support agency under the direction, authority and control of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD[C3I]). It is the central manager of major portions of the Defense Information Infrastructure (DII). The DII will integrate critical warfighter mission and logistic support into a single infosphere that is interoperable and secure.

The Agency began in 1960 as the Defense Communications Agency (DCA), with the goal of consolidating the communications functions that were common to the military departments. The name changed to DISA in 1991 to better reflect its role in providing total information systems support. The Agency is responsible for providing a seamless web of communications networks, computers, software, databases, applications and other capabilities that meets the information processing and transport needs of DOD users in peace and all crises, conflict, humanitarian support and wartime roles.

DISA's main objective is to anticipate and respond to the needs of its customers, the warfighters, by providing them with seamless, end-to-end, innovative and integrated information services which provide a fused picture of the battlefield. It is responsible for planning, developing and supporting command, control, communications, computers and intelligence (C4I) and information systems that serve the needs of the National Command Authorities (NCA) under all conditions of peace and war. It provides guidance and support on technical and operational C3 and information systems issues and coordinates DOD planning and policy for the integration of C4I systems and the insertion of C4I for the Warrior (C4IFTW) leading edge technologies into the DII.

DISA ensures the interoperability and integration of C4I systems such as the Global Command and Control System (GCCS), Global Combat Support System (GCSS), Defense Information System Network (DISN), Defense Message System (DMS), theater and tactical command and control systems, Allied C4 systems and those national and international commercial systems that affect the DISA mission. It also manages the Defense Megacenters (DMCs) and supports the national security emergency preparedness telecommunications functions of the National Communications System (NCS).

DISA will provide support to the warfighters regardless of where they are located, what their mission or what uniformed service or allied nation they belong. It is important that DISA be recognized as the sole provider for the Nation's warfighters in terms of reliable, flexible and affordable information systems support.

For additional information

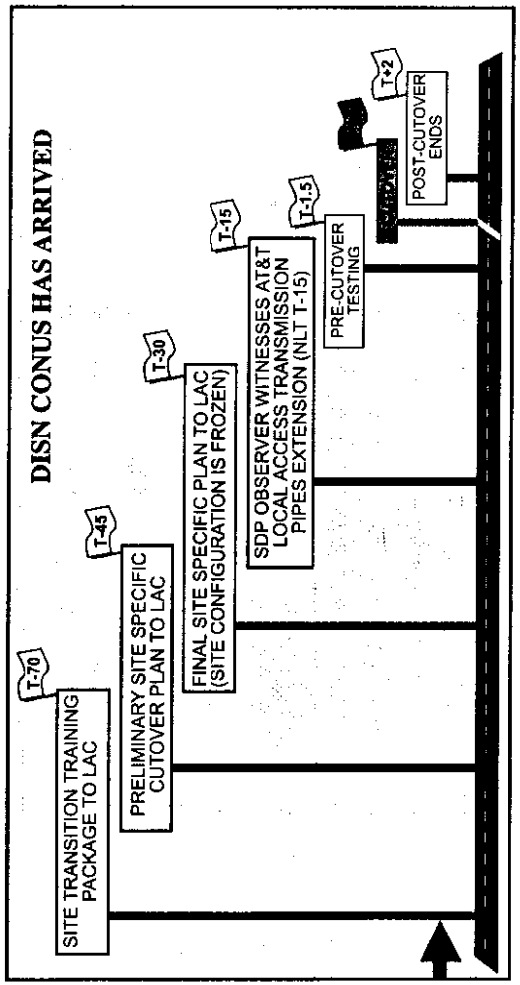
Contact DISA Public Affairs at (703) 607-6900.

(As of June 1997)

Defense Information Systems Agency 701 S. Courthouse Road Arlington, VA 22204-2199

DISN GOALS:

- Provide Broadband Services Supporting Mission Needs
- Implement Security Measures to Protect Information Carried on the Network
- Exercise Positive Control of the Telecommunications Infrastructure



DEFENSE INFORMATION SYSTEMS AGENCY (DISA)

DISA is the DOD agency responsible for information technology and is the central manager of the Defense Information Infrastructure (DII). DISA is responsible for planning and supporting C4ISR that serves the National Command Authority (NCA) under all conditions - peace and war. DISA is subject to the direction, authority, guidance, and control of the Assistant Secretary of Defense C3I and is responsible to the Chairman of the Joint Chiefs of Staff for Operational Matters.

DISA MISSION

"To plan, engineer, develop, test, manage, program, acquire, implement, operate, and maintain information systems for C4I and mission support areas under all conditions of peace and war."

DISN CONUS TRANSITION TEAM CONTACTS

- Army
  - Major Tim Stark, HQDA
    DSN 227-0567, Cmcl (703) 697-0567
    Email: starktl@hqda.army.mil
- Air Force
  - Capt Thomas Becker, AFCA SYXM
    DSN 576-8521, Cmcl (618) 256-8521
    Email: beckert@afca.scott.af.mil
- Navy
  - Chief of Naval Operations
    Major Debra Hall, CNO N61C21
    DSN 664-7840, Cmcl (703) 604-7840
    Email: hall.debra@hq.navy.mil
- Marine Corps
  - Capt Robert de Roziere, USMC Ne/OPSCtr
    DSN 278-2215 3263, Cmcl 784-2215 3263
    Email: deroziere@mqg-smtp3.usmc.mil
- Defense Logistics Agency
  - Jim Livengood, CANI
    DSN 427-3119, Cmcl (703) 767-3119
    Email: james_livengood@hq.dla.mil
- All Other
  - Brigette Thomas, DTT
    DSN 761-6481, Cmcl (703) 681-6481
    Email: thomasb@ncr.disa.mil
- DTT URL:
  - http://www.disa.mil/org/mf39.html
  - DISN Transition Email: disntran@ncr.disa.mil

DEFENSE INFORMATION SYSTEM NETWORK

DISN

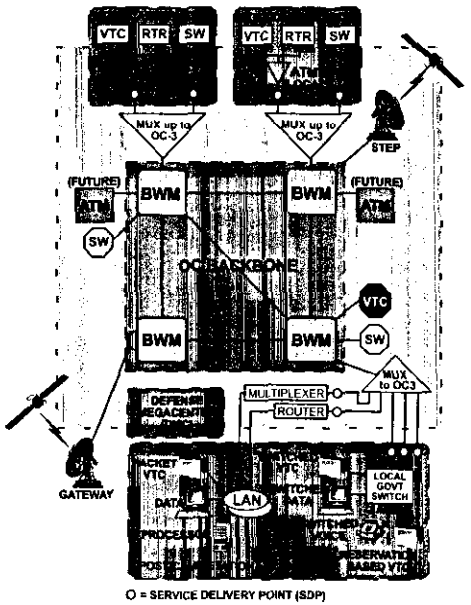
DEFENSE INFORMATION SYSTEMS AGENCY

DISN CONUS TRANSITION

DISN OBJECTIVES:

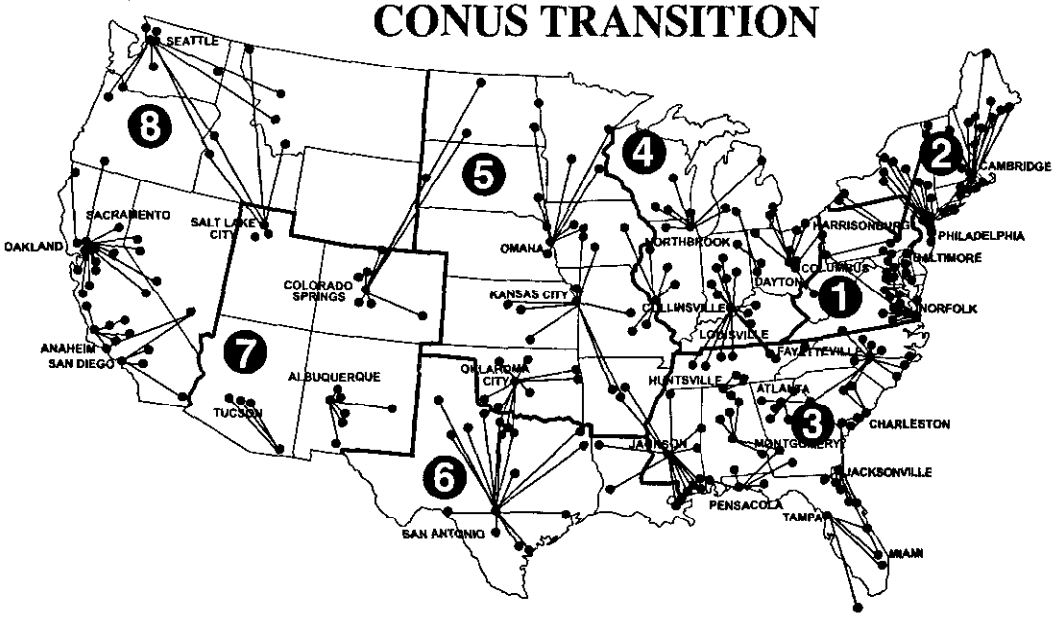
- Satisfy Warfighter Requirements
- Seamless Connections Between Deployed Forces/Home Bases
- Capitalize on Emerging Technologies
- Interoperable with All DOD Services, Government Agencies, and Allies
- Provide Needed Capacity/Connectivity for Warfighter
- Meet Surge Requirements Anytime/Anywhere
- Rapidly Reconfigurable to Meet Warfighter Needs
- Cost Effective, Affordable Services
- Real-Time Management Capabilities Under All Conditions - Peace and War
- Cost Recovered Through Effective Usage-Based Billing

CONUS CONFIGURATION



O = SERVICE DELIVERY POINT (SDP)

CONUS TRANSITION



S/A REPRESENTATIVES

- Assist in Transition Planning, Scheduling, Installation Coordination, and Acceptance Planning
- Identify and Coordinate Transition Actions with Local Area Coordinators (LACs) at the Base, Post, Camp and Station Level

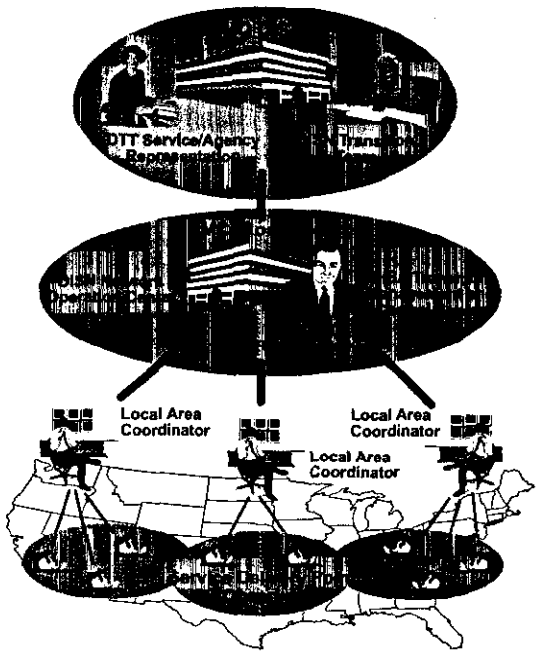
LOCAL AREA COORDINATOR

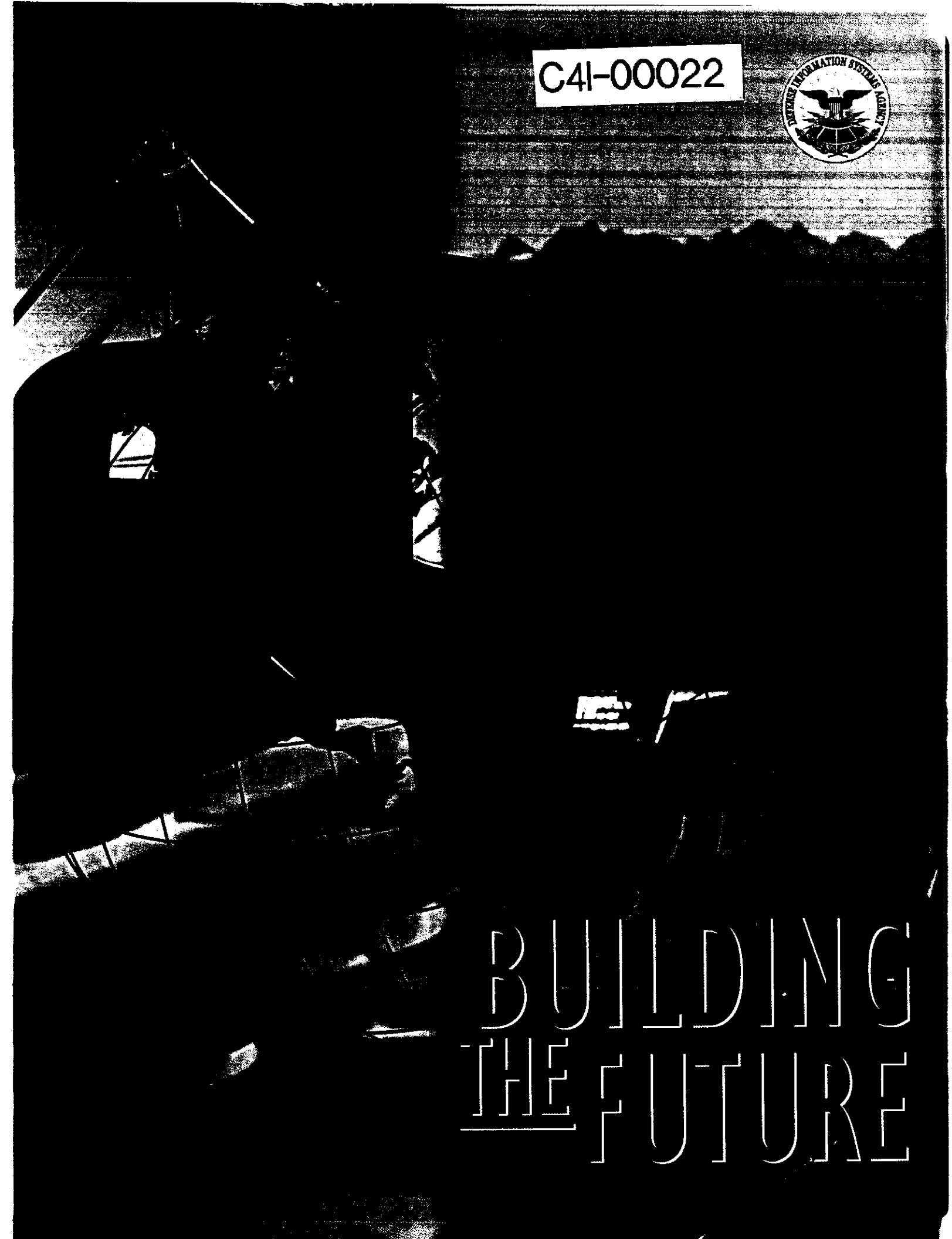
- Provide Local Cutover Assistance
- Review Site Specific Installation Test Plans

SDP OBSERVER

- Provide Service Delivery Point (SDP) Technical Information as Requested
- Record Service Installation and Acceptance Testing
- Submit Implementation Acceptance Test Data to LAC

S/A TRANSITION RELATIONSHIPS





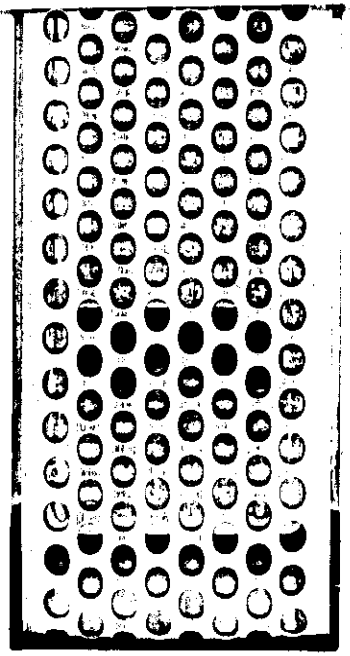
BUILDING THE FUTURE

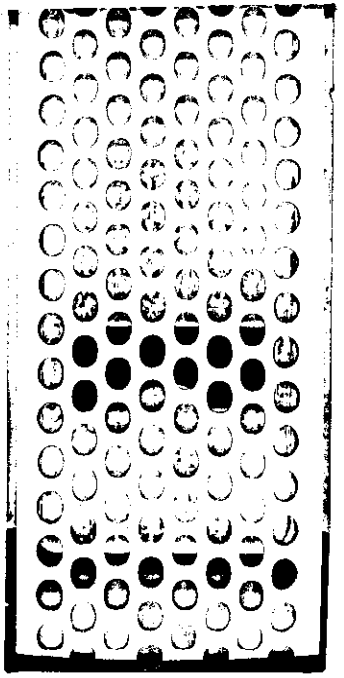
DEPARTMENT OF DEFENSE
DEFENSE INFORMATION SYSTEMS AGENCY
701 S. Court House Road
Arlington, Va. 22204-2199
CODE _____

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE $300

AN EQUAL OPPORTUNITY EMPLOYER

Mr. Howard Benkert
Information Assurance
8283 Greensboro Drive
McLean, VA 22102





Joint Interoperability and Engineering Organization (JIEO)

Summary

JIEO's mission is to ensure interoperability of the Defense Information Infrastructure (DII) and to provide engineering support to warfighters, DISA program and single system managers, Combatant Commands, Services, and Agencies. JIEO provides DOD Information Systems (IS) technical architectures and standards, engineers both hardware and software, and supports the acquisition, implementation, development, and integration of secure IS to meet the needs of DOD users in peace and war. JIEO provides interoperable information technology (IT) services and management of IS engineering services to DOD.

Facts/Discussion

JIEO has five centers and one direct reporting unit:

--Center For Standards (CFS), is the DOD Executive Agent for centralized management of IT standards. The CFS manages the development, adoption, specification, certification, and enforcement of information processing, transfer, and content standards within DOD. CFS also influences the development and adoption by industry of IT standards supporting DOD C4I information systems requirements.

--Center For Systems Engineering (CFSE), provides, on a matrix-support basis, design and developmental engineering and RDT&E for all information transfer and network control systems managed by DISA and constituting the information transport for the DII. CFSE provides an engineering facility for the development, evaluation, applications engineering, demonstration, and technology insertion of all transport technologies used within the DII. CFSE provides specialized support to the National Command Authorities (NCA), Joint Staff, Combatant Commands, the Services, and Agencies. CFSE also performs all of the NCA and Nuclear C3 Systems Engineering responsibilities and functions as stated in CJCSI 5119.01 and manages the special program Project Thrift for the Director, DISA.

--Center For Applications Engineering (CFAE), develops, maintains, and provides operational support for critical operational systems. Operational systems supported include DISA-internal management information systems, Joint Staff applications, DISA developed and/or maintained Global Command and Control System (GCCS) applications, DISA developed and/or maintained Global Combat Support System (GCSS) applications, and other DOD systems assigned. Meets the software needs of OSD, Joint Staff, DISA (including the Chief Information Office (CIO) and other relevant DISA elements), and other

customers as assigned by the Commander, JIEO.

--**Center For Computer Systems Engineering (CFCSE),** implements state-of-the-art software, computer hardware, and data management technologies that provide an efficient, flexible, and secure set of computer systems capabilities that meet the warfighters' requirements. CFCSE engineers the DII, computer systems security, the DII Common Operating Environment (COE) and Shared Data Environment (SHADE), and the Standard Operating Environment (SOE) for the Defense Megacenters (DMCs).

--**Center for Integration (CFI),** provides C4I and DII life cycle support services such as product integration, technical compliance testing, and configuration management (including metrics collection and analysis of hardware/software and network performance), and systems deployment. The OSF maintains a system integration laboratory and hot line, provides on-site installation and engineering assistance, and assists systems engineers in defining operational requirements for supported systems. Provides dedicated CINCs, Services, and Agency support required to plan, engineer, install, train, maintain, sustain, and in some cases operate GCCS platforms to support day-to-day, exercises, special purpose, and contingency mission/operations.

--**DISA Continuity of Operations and Test Facility (DCTF),** provides continuity of operations support to the DMCs and performs integration and testing of GCSS mission applications. The DCTF supports GCSS by building a state-of-the-art prototype model for the DMC of the future. This model facility will then be used to build and test prototype information systems and applications and to implement DII components throughout the DMCs.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of August 1997)

Center for Computer Systems Engineering DII Enterprise Licensing Program

Summary

The DII Enterprise Licensing (DEL) Program provides a mechanism for easily acquiring mainline commericial product software, hardware, and support services at a low cost. The primary mechanism used by the DEL Program is the Integrated Computer Aided Software Engineering (I-CASE) contract - the premier contract for fulfilling the Federal Government's Information Technology needs. The I-CASE contract offers: software, hardware, system and user support services, hardware and software maintenance, and training support to customers.

Facts/Discussion

Software/Hardware: There are hundreds of software products available from leading vendors to support all phases of the software life cycle, from requirements to maintenance. Various platforms, from PCS to mainframes, are also supported. Developers have a wide variety of software options to choose from to support large scale Ada systems and large, complex information systems development. For maintenance and reengineering of legacy systems, a number of analysis and reengineering tools are available. Additionally, a wide array of supporting tools for management, configuration management, database development, testing, quality assurance, metrics, and analysis are available, as well as mainline commercial software applications and models for human resources, logistics, and finance. Of special interest to the DOD community is the availability of all commercial elements of the Defense Information Infrastructure (DII) Common Operating Environment (COE). These offerings include the HP and Sun Unix operating systems, Oracle and Sybase databases, TriTeal's Common Desktop Environment, Transarc's Distributed Computing Environment, and Netscape's full range of web communication products. The flexibility of the contract permits purchasing the software products in small quantities for less than the GSA schedule price and in large quantities (such as for enterprise licenses) at substantial discounts.

There is a wide selection of hardware servers, workstations, peripherals, and networking equipment which is available from the I-CASE contract. This includes a complete line of leading edge products from Sun Microsystems which are priced below GSA schedules. The DEL Program is committed to updating and upgrading the I-CASE offering with new products and versions to ensure that the I-CASE

contract meets current market needs.

System and User Support Services: Provided are the software engineering and environment support, project-unique consulting, technology transfer, process evaluation, and assistance in determining hardware, software and training requirements.

Support services available on the I-CASE contract include the following: product support, integrated software engineering environment implementation planning, migration support, site survey and installation support, change management support, on-site software engineering environment evaluation services, integration and interface support, environment integration and testing, INFOSEC accreditation, information repository data model, and functional requirements system engineering.

Hardware and Software Maintenance/Support: Maintenance may be purchased whether or not the hardware or software was acquired via the I-CASE contract. Software maintenance provides product support, software upgrades (such as bug fixes), and certain software upgrades. Maintenance, training, and annual support are available for most products.

Training: Through the I-Case contract, the DII Enterprise Licensing Program Department can provide the customer with access to a wide variety of vendor-taught software tool training.

Availability/Flexibility: All DOD and Federal agencies can order from the I-CASE contract and there is no need to obtain additional Economy Act determinations. Similarly, there is no need to obtain FAR part 6 justification (see FAR 6.001e) or additional agency paperwork under FAR 17.5 to utilize an Air Force contract. The software can be installed on existing computers, on computers obtained from I-CASE, or from any other source. The contract accepts O&M, Procurement, and RDT&E funds. There are no added administration fees. Ordering and product delivery time frames are short. Contract product-add time frames are short (generally less than 90 days), and when a vendor is added to the contract we include their entire product line.

Enterprise Licensing/Pricing: Enterprise licenses for programs, locations, and agencies can be obtained for most software products. Products on the I-CASE contract are priced below GSA schedules prices for small purchases. Even larger discounts are available on large purchases.

For additional information

Contact DISA Public Affairs at (703) 607-6900 or the DII Enterprise Licensing Program Office at (703) 681-2109.

(As of September 1997)

Defense Information System Network (DISN)

Summary

The Defense Information System Network (DISN) comprises the DOD consolidated worldwide enterprise-level telecommunications infrastructure which provides the end-to-end information transport for supporting military operations, national defense C3I requirements, and corporate defense requirements. DISN provides the primary transmission path to support the Defense Information Infrastructure (DII). DISN features a backbone capability in CONUS with Synchronous Optical Network (SONET) transmission. This transmission is integrated with military and commercial leased communication satellites, switched voice and data services, SONET bandwidth managers, and teleconferencing services.

Facts/Discussion

In July 1995, DISA announced its strategy for the next generation global telecommunications infrastructure that would support the Nation's Warfighters worldwide. As a result, DISN would replace expiring contracts and aging systems with a global approach designed to take maximum advantage of industry capabilities and evolving technologies. The goal architecture represented a graceful technological evolution from the use of DOD-owned and operated networks and systems to commodity services where possible.

The DISN strategy will consolidate more than 100 independent DOD networks into a single, integrated, cost effective, efficient, common-user global "infosphere," a grid that will provide connectivity on demand anytime, anywhere. This will help alleviate the problem with individual legacy communications systems which are not effectively integrated and often non-interoperable. Today, these disparate systems impede or even prevent the exchange of information between warfighting commands and units. DISN serves as the evolving DOD worldwide protected network allowing Warfighters to "plug in" and "push or pull" information in a seamless, interoperable and global battlespace.

DISN is a dynamic network, with the capability to accommodate emerging new or improved technologies that better serve the unique communication needs of the Warfighter. DISN provides seamless and interoperable information transport across strategic and tactical networks supporting Joint Task Forces and Combined Task Forces, as well as the telecommunications networks of non-defense agencies.

DISN will provide the transmission and switching of voice, data, video, and point-to-point bandwidth services for wide area, local area, metropolitan area, and long-haul networks.

DISN will use available commercial products and services, while providing DOD with the degree of network control necessary to ensure rapid response to the Warfighters. DISN integrated voice/imagery and data information transport will be transparent to the Warfighters, facilitate the management of information resources and be responsive to national security and defense needs under all conditions in the most efficient manner.

In early 1995, the Joint Chiefs of Staff (JCS) validated a Mission Need Statement (MNS) which realigns priorities from simple business-case services to a more secure and government controlled network of commercial switching nodes and leased transmission services. This focuses C4I more directly for the Warfighter.

In early 1996, the JCS issued a Capstone Requirements Document which clearly segments DISN into three distinct blocks. These blocks are base level, long-haul, and deployed. All blocks are to be implemented as fully interoperable blocks, but by different organizations, with the technical oversight of DISA. The Services will implement DISN on their respective bases, DISA will implement the long-haul block, and different Services or Agencies will be designated to jointly implement the deployed block.

Since July 1995 when the strategy was announced, DISA has awarded all four initial DISN contracts. The first contract, DISN Support Services - Global (DSS-G) contract, was awarded to Boeing Information Services, Inc. The DSS-G serves as the network's technical management support vehicle. The second contract, DISN Switched/Bandwidth Manager Services (DS/BMS-C), was awarded to MCI Telecommunications Corp and covers the continental United States (CONUS). In addition to supporting the vast majority of CONUS, this contract covers overseas traffic that originates or terminates in the 48 contiguous states.

The third contract, DISN Transmission Services - CONUS (DTS-C), was awarded to AT&T Government Markets. This contract will provide backbone and access area transmission services at T-1 and above bandwidth rates. The fourth contract, DISN Video Services - Global (DVS-G), was also awarded to AT&T Government Markets. AT&T will provide multi-vendor interoperability and dedicated video services including secure and non-secure, point-to-point and multi-point bridging, a reservation/scheduling system, video services management and monitoring, and provisioning and user-site network interface equipment.

DISA has also awarded the DISN Hawaii Information Transfer System (HITS) contract to AT&T Government Markets. This provides wide-area and local networking services to DOD facilities within the State of Hawaii.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of June 1997)

Defense Message System (DMS)

Summary

DMS consists of all the hardware, software, procedures, standards, facilities and personnel needed to exchange electronic messages among organizations and individuals in the Department of Defense (DOD) whether at home base, while traveling or when deployed. DMS will provide a common messaging environment that is flexible and interoperable between the Military Services, Agencies, Joint Staff, Federal Agencies, our Allies, and the public.

Using the global Defense Information System Network (DISN) transmission system and supporting local/tactical infrastructure capabilities, DMS provides electronic messaging, directory, security, and management services for DOD organizations and individuals.

Goals and Development

For the past 35 years, AUTODIN has provided DOD with unprecedented messaging support. Although the system has undergone numerous enhancements, its basic framework is 1960's proprietary technology; consequently, it cannot be easily upgraded to support today's information requirements.

When the DMS program began, it established two keys goals: 1) develop a system that reduced the high operation and maintenance costs associated with AUTODIN, and 2) improve messaging support to the warfighters.

To achieve these and other goals, the DMS program turned to commercial industry for solutions. Rather than build another proprietary system with enhanced capabilities (in essence, a new and improved AUTODIN) the program sought commercial product offerings to meet the full range of DOD's needs. The program first established a baseline from which proposed DMS costs and benefits could be measured. Using validated requirements and established commercial technology objectives, a DMS target architecture was defined with an accompanying implementation strategy to evolve from the baseline to the target.

Acquiring the System

In January 1993, the Defense Information Systems Agency (DISA) was tasked to lead the continued development of an integrated system that provided advanced messaging and directory services, and phase out the AUTODIN system. The DMS "continuous evolution" approach has kept the program in step with commercial industry trends.

The DMS program employs an innovative acquisition strategy designed to influence development of mainline commercial products while maintaining maximum competition and acquisition flexibility. Through this acquisition, vendors are encouraged to provide commercial

product solutions to meet DOD messaging and directory service needs. These solutions, which require the incorporation of international standards, ensure essential characteristics that include connectivity, interoperability, accountability, reliability and security. In keeping with common commercial practice, major commercial vendors provide these features as "add-ins" to their core commercial offerings.

Track I of the dual-track DMS acquisition is designed to acquire the baseline DMS secure, accountable, and reliable "system" consisting of the managed global infrastructure and initial DMS compliant user components. Execution of Track I began when DOD awarded an Indefinite Delivery, Indefinite Quantity (IDIQ) acquisition contract for DMS-compliant products and services to Lockheed Martin Federal Systems (LMFS) in May 1995.

An independent compliance test and evaluation program, administered by the DISA Joint Interoperability and Test Command (JITC), has been developed to test and certify Track I products from the LMFS contract as well as Track II products from other vendors.

DMS Today

On 3 June 1997, 13 Track I products from the LMFS contract completed DMS compliance Test and Evaluation (CT&E) and were posted to the DMS Certified Compliant Products List (CCPL). These products, comprising the baseline DMS "system," serve as "reference implementations" of DMS compliant products as Track II products enter the compliance test and evaluation process. Track I compliant products are from CommPower, Enterprise Solutions, Ltd, LMFS, Lotus Development, Microsoft, and Xerox. Novell is the first Track II vendor to enter the CT&E process and more than 20 additional vendors have expressed interest in submitting their products for DMS compliance testing.

Initial Operational Test and Evaluation (IOT&E) of the initial DMS system (Release 1.0) commenced on 28 May 1997 and will continue through July. As this basic DMS capability completes operational testing, the next DMS release (1.1) is under development and scheduled to enter streamlined compliance testing in September 1997. As operational experience is gained, problems will be resolved and additional functionality added through additional DMS releases approximately every 6 months. Concurrent testing of each new release and development of the following release is a necessary aspect of maintaining currency with commercial technology.

Simultaneously, the Joint DMS Community is defining flexible DMS implementations that allow DOD users and organizations to take full advantage of features such as collaborative computing that DMS compliant commercial products offer in conjunction with their messaging features. The ultimate DMS objective is to remain firmly within the commercial technology mainstream while ensuring satisfaction of validated DMS requirements.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of June 1997)

Information Security (INFOSEC)

Summary

INFOSEC is the measures and controls that safeguard and protect an information system from unauthorized disclosure, modification or destruction from such threats as hackers, terrorists and foreign governments. The Defense Information Systems Agency, (DISA) as central manager of the Defense Information Infrastructure (DII) and in joint cooperation with the National Security Agency (NSA), defines INFOSEC requirements and implementation into the DII. The Defense Intelligence Agency (DIA) supports these activities with threat assessments.

Facts/Discussion

The DII is a seamless web of communications networks, computers, software databases, applications, facilities and other capabilities that meet the Department of Defense's (DOD) information processing and communications needs. Information systems cannot be protected with a single mechanism. DISA must ensure that the DII contains the adequate protection against attack by using a layered defense.

Under the Multilevel Information Systems Security Initiative (MISSI), NSA is developing a complete suite of security products which include the FORTEZZA family of crypto cards, firewalls and multilevel security guards/gateways which DISA is implementing to protect the DII. DISA is working to ensure that information security is integrated into all of its programs from the beginning.

The Global Operations and Security Center (GOSC) consolidates the functions of the Global Control Center and the Automated Systems Security Incident Support Teams (ASSIST) into one organization. This consolidates all aspects of security into the day-to-day management and operation of the networks supporting the Department of Defense. The center monitors, detects, and reacts to disruptions in the infrastructure. The center also includes daily operation of the Vulnerability Analysis and Assessment program (VAAP). This program provides an evaluation of the overall security posture of the DII by way of intrusion penetration testing. The Defense Intrusion Analysis and Monitoring Desk (DIAMOND) is located in the center and provides advanced analysis of intrusion data and network sensors looking for unauthorized activity. The GOSC also provides DOD-wide support for the detection, analysis and removal of malicious code (more commonly known as viruses, logic bombs, etc.).

The INFOSEC Program Management Office (IPMO) consolidates the acquisition, implementation, integration and dissemination of INFOSEC products and services into the DISA pillar programs (e.g., DISN, DMS, GCCS, and GCSS) and other DOD systems and activities. The IPMO coordinates with the CINCs, Services and Federal Agencies to determine requirements and develop standardized INFOSEC tools, methods, and training and awareness products, which help to ensure the confidentiality, integrity and availability of warfighter information systems. The IPMO provides INFOSEC technical support functions to include INFOSEC certification, connection approval and compliance validation of connections to the DII. The IPMO also manages development and fielding of standard multilevel security capabilities supporting CINC, Service and Agency C4I requirements.

DISA supports Information Warfare - Defense activities of intelligence organizations, the CINCs Services, other Federal Agencies, and the private sector.

(As of February 1997)

Center for Computer Systems Engineering Information Resources and Customer Service

Summary

The Information Resources and Customer Service (IRCS) division provides accurate, efficient and timely information and support for the Defense Information Infrastructure (DII) products and services. The current DII products and services are: Ada, Asset Distribution Standard Operating Environment (SOE), Data Engineering (formerly SHADE), Software Enterprise Licensing (SEL); Common Operating Environment (COE), and Systems Security Engineering.

Facts/Discussion

IRCS operates the Center for Computer Systems Engineering (CFCSE) Information Clearinghouse which prepares and distributes: program brochures, compact disks, DII training materials and reference manuals, electronic product flyers, fact sheets, information diskettes, multimedia presentations, quarterly newsletters and news briefs.

The IRCS supports the Web-based DII COE Management Overview Training and the on-site DII COE Technical Workshop. Also, IRCS provides a product specific referral service and Internet access to the DII products and services.

How we do our business

- DISTRIBUTE current information about the DII COE products and services;
- INITIATE business partnerships to support the DII COE products and services;
- INFORM customers at seminars, trade shows, and other events about the DII COE products and services;
- PROVIDE product specific referral services and Internet access to the DII COE products and services;
- SUPPORT DII COE Training requirements in the classroom and on-line; and
- RESPOND to customer inquiries via our DII COE Hotline at **1-800-738-7379**.

For additional information

Contact DISA Public Affairs at (703) 607-6900, the DII COE Hotline; or access our Web site at http://dii@sw-eng.falls-church.va.us/CSEIC.

(As of October 1997)

Defense Information Systems Agency 701 S. Courthouse Road Arlington, VA 22204-2199

Center for Computer Systems Engineering Standard Systems Engineering

Summary

The Standard Systems Engineering Department provides DISA with technical design and schedule on efforts to migrate from the Unisys platform to the Defense Information Infrastructure (DII) Common Operating Environment (COE). The current goals are to phase out proprietary platform, *ramp up* the Defense Megacenter (DMC) DII COE supporting infrastructure, and assist customers in migrating applications to the DII COE at DISA facilities.

Facts/Discussion

The Standard Systems Engineering Migration Strategy Options include rehosting and reengineering. Rehosting advantages include greater interchangeability and portability of applications (COE), greater facilitation of centralization and system optimization, and greater improvement in efficiency. Other advantages include technological enhancements, allowance for later reengineering for Y2K compliance, and provision of scalability and modularity for new workloads.

Standard Systems Engineering has implemented Unisys Migrations to the DII COE. Presently, there are 71 Unisys Platforms, 20 Million Lines of Code, 8 DMCs, 2 OCONUS Sites, and 4 major customers. CFCSE has placed its focus on the Air Force/Defense Finance and Accounting Service (AF/DFAS) Standard Base Level Computing (SBLC) Maintenance, Supply, Personnel, Finance, Budget and Operation Support (85 percent total AF/DFAS).

Through the department's efforts, the DMCs have become DII compliant implementing COE migration strategies. The migration steps include selecting candidate migration systems, documenting current environment, identifying target environments, identifying migration risks, assigning roles and responsibilities, performing cost benefit analysis, developing system migration schedules; and migrating the systems.

For additional information

Contact DISA Public Affairs at (703) 607-6900 or the Standard Systems Engineering Department at (703) 681-2233.

(As of September 1997)

Center for Computer Systems Engineering Data Engineering

Summary

The Data Engineering Department's products and services are focused on the C4I for the Warrior (C4IFTW) vision to perform "Any Mission, Any Time, Any Where." DISA's mission is to make C4IFTW a reality.

Throughout DOD, there are critical mission requirements in command and control, intelligence, procurement, logistics, personnel, finance, etc. These mission requirements translate into both the application and data needs of the department's customers.

The Data Engineering department is focused on database segments and data access services which the customers, the proponent of these systems, can place on a server to support their mission needs. The department's goal is to help customers field their databases and data assets more effectively, cost efficiently, and easily by providing the products and services needed for the sharing of data and a way for customers to access and store it. The department is convinced that data sharing requires at least three things be in place: rules and tools, reusable data components, and participation between functional proponents, program offices and system administrators.

Facts/Discussion

First are the rules and tools to promote data sharing. For common operating environment developers, this means customers need engineering rules for building and integrating system components, including data and databases. These rules are in the Integration and Runtime Specification (I&RTS). This specification describes how reusable system components are built and integrated as segments (i.e., account group, applications, COTS/GOTS, data, and databases). Having rules is only one step. Because rules can be misinterpreted, customers also need tools--tools that can help to support the development, maintenance, and implementation of reusable system components. Under the shared data environment, that means tools to support the development, maintenance, and implementation of data and database segments.

Second are the reusable data components to promote data sharing. Customers first need a data management system which is easy to install and implement. In the COE environment, those are Oracle, Sybase, Informix, and MS Access. Next, customers

need consistent data structures that can be shared. This includes tables, table layouts, and the actual data values. Finally, data components are needed that will provide easy access to data resources. For example, customers need tools to support browsing, replication, and decision support requirements (e.g., web browsers, Omni Replicator, Brio, and Cognos).

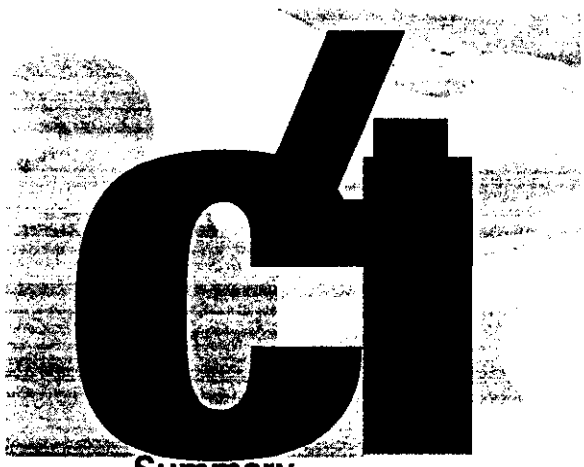
Third is participation from customers who are interested in improving the ways that they share data to promote data sharing. This participation can come from functional proponents, program managers for systems, developers, the COE technical working groups that provide oversight on the common support applications, and the infrastructure services that make up the COE.

Most importantly, customers should understand what DII COE Data Engineering is not about: it is not about building one big data server, nor is it about taking over servers or their ownership. The Data Engineering Department is in the business of helping customers field their databases and data assets more effectively, efficiently, and easily.

For additional information

Contact DISA Public Affairs at (703) 607-6900 or the Data Engineering Department at (703) 681-2394.

(As of October 1997)



Engineering and Interoperability Directorate (D6)

Summary

D6 is responsible for information systems engineering and interoperability support to all DISA programs, Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD[C3I]) directed initiatives, and other Director, DISA-coordinated efforts. D6 is "dual hatted" as the Commander of the Joint Interoperability and Engineering Organization (JIEO) with full program, policy and resource control. Through JIEO, D6 provides information technology support over the full range of warfighter-to-mission support systems and components of the DISA-managed Defense Information Infrastructure (DII).

D6 is responsible for providing Department of Defense (DOD) information systems architectures and standards and hardware and software engineering to support the acquisition, implementation and integration of secure information systems that meet the needs of DOD users in peace and war.

Facts/Discussion

D6 serves as the principal staff officer on all matters concerning the engineering and interoperability of the Defense Information Infrastructure (DII) and Defense Information System Network (DISN). D6 is responsible for ensuring the provision of Information Systems (IS) engineering and interoperability support to all DISA programs, directed under the ASD (C3I) Information Management initiatives, and for such other programs or efforts directed by the Director, DISA.

D6 evaluates, engineers, and ensures delivery of an integrated Global Combat Support System (GCSS), combining infrastructure capability with combat support applications of the Services, Agencies, Combatant Commands, Joint Staff, and Principal Staff Assistants in the Office of the Secretary of Defense (OSD). D6 integrates counterdrug specific applications into the DII, executes an architectural development program leading to interoperability across law enforcement agencies, and provides life cycle support for ongoing DISA counterdrug programs.

D6 has four divisions:

--**Resource Management Division,** is the principal advisor to D6 on all financial management, personnel, manpower, foreign military sales, fiscal year corporate plans, budget planning and execution, and resource issues. It provides oversight and direction on contract administration, financial planning, and execution matters. Executes the DISA information program across D6/JIEO, ensuring that Information System Security (ISS), Information Management (IM), and Information Resource Management (IRM) functions are carried out effectively and efficiently and in accordance with applicable laws and regulations.

--**C4I Engineering Management Division,** ensures that C4I engineering contributes to the integration of command and control, intelligence, and combat support capabilities to achieve a flexible, modular, effective and efficient information infrastructure for the warfighter. Provides engineering management for the evolution of the Global Command and Control System (GCCS) and GCSS; provides effective business reengineering procedures, methods, techniques, tools, and services for DISA, DOD, and other government agencies through collaborative techniques and tools; manages the integration of command, control, and intelligence capabilities through the use of state-of-the-art hardware and software solutions; provides support to the Joint Staff, Joint Warrior Interoperability Demonstration (JWID) Lead Service, and the JWID Host CINC in yearly demonstrations of C4I leading edge technology in accordance with the goals of C4I for the Warrior; provides systems engineering for modification and/or improvements of the command and control information systems residents in any National Military Command System (NMCS) command center; provides engineering expertise for resolving command center technical issues; and provides the engineering for the evolution of the Electronic Commerce/Electronic Data Interchange (EC/EDI) capability for DOD.

--**Office of the Technical Director,** provides technical leadership for the enhancement and implementation of the DII with particular emphasis on interoperability and horizontal integration. This is accomplished through the Chief Engineers Panel which promotes teamwork for all DII engineering initiatives within DISA and stimulates technical exchange by focusing on horizontal integration across major components of the DII. Other organizations fall under the Office of the Technical Director such as the GCSS Chief Engineer organization which develops, integrates, tests and fields a DII Common Operating Environment (DII COE) compliant system for transportation, medical, logistics, personnel, finance, acquisition and other combat support applications; the GCCS Chief Engineer organization which develops, integrates, tests and fields a DII COE compliant system for Command, Control, and Intelligence applications; the DISA/DARPA Joint Program Office which facilitates the transfer of DARPA advanced technology from R&D to Joint Service operational deployment; and the Technical Policy and Interoperability organization which assesses all C4I requirements documents to ensure compatibility, interoperability and technical integration of DOD Information Systems. This organization also provides support to the Major Automated Information System Review Council (MAISRC), the DII COE Configuration Review and Control Board (CRCB) and the Joint Staff in the development of Joint Publications/Doctrine for the employment of C4I Systems.

--**Counterdrug Integration Division,** serves as the sole focal point and office of record for all tasking actions assigned to DISA and the National Communications System (NCS) supporting the National Drug Control Program.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of August 1997)

Defense Information Infrastructure (DII)

Summary

The DII is the web of communication networks, computers, software, databases, applications, weapon systems interfaces, data, security services, and other services that meet the information processing and transport needs of DOD users across the range of military operations. It implements the C4I For The Warrior (C4IFTW) vision of an user-driven infrastructure through which warfighters and other DOD users can quickly share needed information from any location, at any time using secure voice, text, and video services. The DII will allow warfighters to maintain information superiority by presenting a fused, real-time, true representation of the three dimensional battlespace.

Facts/Discussion

The DII will allow U.S. Forces to meet the needs of the National Military Strategy: U.S. Forces must be able to project power from Continental U.S. bases, sanctuaries and in-theater locations in times of conflict, plus support up-to-the-minute peacetime missions.

The DII will operate as a collection of distributed, heterogeneous information systems. It will range from DOD applications implemented at central locations, to base-level or end-user applications on desktops or in tactical environments. The infrastructure requires collaborative development reflective of its cooperative ownership among the Office of the Secretary of Defense (OSD), the Joint Staff and individual services and agencies.

The current DII consists of many elements, much like a puzzle in which each piece is crucial to the overall picture. These elements build on and include a foundation of integration and technology support. It is important that the DII evolve to support new and existing missions, to provide new capabilities, and to introduce new technology.

The DII encompasses:
--sustaining base, tactical, DOD-wide information systems. and Command, Control, Communications, Computer,m and Intelligence (C4I) interfaces to weapons systems
--the physical facilities used to collect, distribute, store, process, and display voice, data, and imagery
--the applications and data engineering practices (tools, methods, and processes) to

build and maintain the software that allow C2, intelligence, surveillance, reconnaissance, and mission support users to access, manipulate, organize, and digest proliferating quantities of information.
--the standards and protocols that facilitate interconnection and interoperation among networks and systems and provide security for the information carried.
--the people and assets which provide the integrating design, management and operation of the DII, develop the applications and services, construct the facilities, and train others in DII capabilities and use.

The Defense Information Systems Agency (DISA) works with the CINCs, Services and other Agencies to develop the DII Master Plan for ASD(C3I). The DII Master Plan is a living document that establishes the common DOD vision for the DII, identifies current and future elements, defines DII participants' roles, responsibilities and relationships, and identifies the relationships and interdependencies of key initiatives.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of June 1997)

Center for Computer Systems Engineering Systems Security Engineering Department

Summary

The DISA Systems Security Engineering Department (SSED) provides INFOSEC architecture and engineering support for major DISA and DOD information technology programs. The highest priority of the organization is to provide INFOSEC engineering support to the DISA Pillar Programs: Global Command and Control System (GCCS), Defense Information System Network (DISN), Defense Message System (DMS), and Global Combat Support System (GCSS).

Security is an essential requirement of all information networks. Today's warfighters, from the foxhole to the National Command Authority, depend on strong security technology to protect their valuable information. SSED supports the warfighter by providing the necessary engineering support that enables the five major security services (Availability, Identification and Authentication, Confidentiality, Integrity, and non-Repudiation), to be engineered into today's modern information systems.

Facts/Discussion

SSED's mission is to provide the systems security engineering support necessary to ensure secure interoperability capabilities to all DOD Command, Control, Communications, Computers, and Intelligence (C4I) Information Systems from inception through fielding. The purpose of this organization is to provide security engineering assistance to DOD Service and Agency customers, by providing the security expertise and support necessary to incorporate the appropriate security features into information systems throughout the life-cycle of the system. As security engineers, the SSED recommends INFOSEC Automated Information System (AIS) Technology Standards to DII programs, and is influential in both commercial and government security product development.

With the initial design completion of a Public Key Infrastructure (PKI), the alpha release of the Windows NT configuration wizard, the final analysis of the JCALS security architecture, and an initial design and risk assessment for a Virtual Private Network (VPN) for the Defense Travel System (DTS), SSED continues to provide dedicated security engineering support to our customers. Our customers include DISA directorates: D6/JIEO, D2/C4 & Intelligence, and D3/Operations; Program

Managers for Joint Computer Aided Logistic System (JCALS), Global Combat Supply System-Air Force (GCSS-AF), Standard Procurement System (SPS), Global Command and Control System (GCCS), and Global Transportation Network (GTN); Military Intelligence Group; Navy Logistics Integrated Product Team; Electronic Commerce/ Electronic Data Interchange (EC/EDI); Information Security Program Management Office; and the Joint Program Office, Defense Advance Research Program Agency (DARPA); and Commanders in Chief (CINCs).

The number one barrier to information security is education. Despite the numerous reports of information system attacks, convincing customers that security should be a major concern in the design stages of an information system is still a big part of the job. It is important for customers to realize that every computer system is vulnerable to attack. Security policies and products can only reduce the likelihood that an attack will actually be able to penetrate system defenses. While engineering the security aspects of a system, focus should be placed on risk management, vice risk avoidance --there is no such thing as a completely secure information system.

For additional information

Contact DISA Public Affairs at (703) 607-6900 or the Systems Security Engineering Department at (703) 681-2340.

(As of October 1997)

Center for Computer Systems Engineering Software Data Architecture Division

Summary

The Software Data Architecture Division's mission is to define and deliver the Defense Information Infrastructure (DII) Common Operating Environment (COE). The DII COE provides the ubiquitous foundation for all DII system architectures to enable operational realization of the Command, Control, Communications, Computers, and Intelligence for the Warrior (C4IFTW) vision. The DII COE enables interoperability by providing engineered methods, components, and tools to build systems which allow the warfighter to receive, transmit and interpret information consistently.

Facts/Discussion

The DII COE is a fundamentally new approach emphasizing both software and data reuse and interoperability. The DII COE provides an innovative framework for designing and building military systems. Because it reuses software contributed by service/agency programs, it utilizes field-proven software for common functions. The engineering procedures for adding new capabilities and integrating systems are mature and have been used for several production releases. The DII COE provides a strategy for fielding systems with increased interoperability, reduced development time, increased operational capability, minimized technical obsolescence, minimal training requirements, and minimized life-cycle costs.

The goals of the Software Data Architecture Division are to continue meeting user requirements and expectations through well managed, timely, and incrementally delivered, superb software products.

Software products encompass the following:

- An architecture and approach for building interoperable systems
- An environment for sharing data between applications and systems
- An infrastructure for supporting mission area applications
- A rigorous definition of the runtime execution environment
- A reference implementation on which systems can be built
- A collection of reusable software components and data
- A rigorous set of requirements for achieving DII compliance
- An automated toolset for enforcing COE principles and measuring

DII compliance

- An approach and methodology for software and data reuse
- A set of application programming interfaces for accessing COE components
- An electronic process for submitting/retrieving software and data to/from the DII repository

The DII COE allows the development, integration, migration, and implementation of mission applications into the DII. It provides a common environment in which mission applications may be introduced and run. The end result is a consistent approach to software development and integration, reliability and cost savings resulting from the reuse of field-proven software, the introduction of commercial software capabilities into the warfighter's arsenal, additional economies from eliminating duplicative functionality, and the means to achieve information understanding across multiple domains.

For additional information

Contact DISA Public Affairs at (703) 607-6900 or the Software Data Architecture Division at (703) 681-2307.

(As of September 1997)

Global Combat Support System (GCSS)

Summary

The C4I for the Warrior (C4IFTW) concept is committed to meet the warrior's information requirement to achieve victory for any mission, at any time, and at any place. C4IFTW is the vision and roadmap for creating an integrated combat support picture for the warfighter.

GCSS is the final piece of the C4IFTW concept. It is a demand-driven, joint warfighter-focused initiative to accelerate delivery of improved combat support capabilities. Using the same approach, methodology, practices, tools, and integration procedures as the Global Command and Control System (GCCS), GCSS is an initiative that integrates existing combat support systems to gain efficiency and interoperability in support of the warfighter. GCSS will provide the warfighter with a fused, real-time combat support view of the battlespace.

Facts/Discussion

Currently, the Joint Task Force has stovepiped information systems in logistics, personnel, engineering, finance, acquisition, and health services. GCSS will eliminate these stovepipe systems and develop a shared information database access via a single computer.

One of the components of GCSS is the Electronic Commerce (EC)/Electronic Data Interchange (EDI) infrastructure initiative. This initiative enables the warfighter to electronically access goods and services in a timely and efficient manner via the Electronic Commerce Infrastructure (ECI).

GCSS will create a technical environment and process to economically integrate existing computer-based systems software and hardware using the common operating environment (COE) and shared data environment (SHADE). It will also expand the GCCS COE to accommodate combat support applications and will also provide "split base-reachback" capabilities from the foxhole to the sustaining base to allow the warfighter to be "deployed" by electronic means.

GCSS provides on-line connectivity to NIPRNET/SIPRNET web and access to applications and data. GCSS will have heavy user participation, and through incremental improvement will evolve to hardware independence and interoperability.

GCSS goals are to:

--Provide the warfighter reachback to combat support capabilities and personnel that remain in garrison.
--Provide a combat support infrastructure that is responsive to joint mission support needs.
--Provide a flexible and adaptive open computing environment.
--Enable interoperability and integration across combat support areas and from combat support to the combat environments.
--Integrate and implement an information infrastructure that provides end-to-end information connectivity and access.

GCCS and GCSS both need the Defense Information System Network (DISN) and the Defense Message System (DMS) to complete C4IFTW. GCSS will rely on all components of the DISN for information transport services including voice, text, and imagery. DMS provides the warfighter a secure, reliable, and accountable writer-to-reader messaging infrastructure at reduced cost.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of June 1997)

Center for Computer Systems Engineering DII Asset Management Department

Summary

The DII Asset Management Department provides infrastructure to Department of Defense (DOD) customers to include: mechanisms, guidance, and processes for the electronic population, storage, dissemination, management, and control of Information Assets supporting Defense Information Infrastructure (DII) compliant DOD mission applications.

Facts/Discussion

The DII Asset Management Department in the Center for Computer Systems Engineering provides the DII Asset Distribution (DAD) infrastructure, an umbrella system for data and software repository access and distribution to include:

- Web Services
- Defense Data Dictionary System (DDDS) and the Personal Computer Access Tool (PCAT), a PC version of the DDDS
- Segment Repository
- End User Support for Suite of Tools
- Consumer Information on Tools

The DAD is the much needed distribution system to get quick delivery of those assets required to meet the mission, whether it is applications for the warfighter or COE, data, and/or application tools for the developer. The system also includes a tracking system to identify the users who request distribution and to identify which systems are accessed.

The department is committed to identifing and implementing low cost commercial off the shelf (COTS) solutions to meet the needs of the customers. Work with DOD customers to ensure rapid distribution of their assets includes:

- DII Common Operating Environment (COE)
- Global Command and Control System (GCCS)
- Global Combat Support System (GCSS)
- Software Enterprise Licensing (SEL)
- Defense Message System (DMS)

- Shared Data Environment (SHADE)
- Information Security (INFOSEC)

Benefits to the DOD customer are:

- Timely (within minutes) access to the assets needed. Currently the assets are packed and shipped to the customer within several days to three months.
- Reduced Distribution Costs. As an example, the cost of packing and shipping the COE to each customer exceeds that of distributing it electronically.
- Increased Customer Satisfaction. The customer (warfighter and developer) will have the asset(s) when they need it.
- Increased mission effectiveness. The customers/users will meet their time lines because of instant access to the required assets.
- In addition to distribution, the department updates and maintains the DDDS and the PCAT, which are projected to be distributed on the web.

The DDDS currently contains over 28,000 data elements with 10,869 approved and over 1,250 currently under functional and technical review. The DDDS also has over 1,400 users worldwide from all DOD agencies.

PCAT was developed for users who cannot gain access to the DDDS because they are in a secure environment, because communications lines are not available, or because there are restrictions which makes access to the DDDS not practical. To date, more than 800 copies of PCAT have been distributed to registered users in the DOD Data Administration community.

Future plans to meet customer demands include refreshed technology, and increased capability and functionality of components, tools, guidance, and documentation.

For additional information

Contact DISA Public Affairs at (703) 607-6900 or the DII Asset Management Department at (703) 681-2166.

(As of October 1997)

ATM ANYTIME! ANYWHERE!

EDGESPAN ATM SERVICES

ATM ANYTIME! ANYWHERE!

Today's World Presents New Challenges:

Eliminate Multiple Dedicated Networks:

- *Less than full utilization of bandwidth in existing circuit based networks*
- *Additional locations require increased connectivity raising private line network costs*

Preserve Legacy Equipment Investment:

- *Existing network represents a considerable investment that is in service and must operate over new networks*

Requirement for High Bandwidth Applications:

- *Emerging applications require greater bandwidth*
- *Today's LAN speeds reach operating speeds of 100 mbps*

Emergence of Multimedia Applications:

- *New applications demand a mixing of traffic types for voice, video, data, and imagery*

Improve Communication among Joint Task Force Members:

- *Provide global reachback capability to support services in CONUS*
- *Creation of communication systems where none may exist*

ATM Addresses These Challenges By:

Reducing Cost of Networking:

- *Better utilization of bandwidth is realized because circuits are not standing idle while other networks are suffering congestion. ATM "mixes" the traffic to optimize the load.*
- *Additional locations can be added without reconfiguring the entire network.*

Protecting Investment in Legacy Systems:

- *Legacy systems can be managed and planned for replacement over a longer period of time. Existing systems can be interfaced to ATM transport networks without having to replace the working system.*

Supporting Higher Bandwidth Applications:

- *ATM is viewed as the gateway to high speed transport now and in the future. Access speeds are already operating at OC-3 (155 MB); with OC-12 (622 MB) and OC-48 (2.4 GB) planned for the future.*

Accommodating Multimedia Applications:

- *As new applications require the simultaneous use of voice, data, video, and imagery in various combinations, ATM is the transport technology that can merge these data streams.*

Emerging as an Internationally Accepted Protocol:

- *COTS communication platforms designed around commonly accepted network standards*
- *Reduces requirement for multiple protocol conversions*

Yurie

AT&T

AT&T EdgeSpan LDR ATM Service

AT&T Yurie

FACT SHEET

AT&T's EdgeSpan Limitless Data Rate (LDR) ATM service supports the Warfighter with a deployable end-to-end ATM solution.

EdgeSpan LDR ATM gives end-users of any size, at any location, the capability to consolidate multiple traffic types (voice, date, video) onto high speed ATM networks to take advantage of ATM efficiencies.

EdgeSpan, which is based on Limitless Data Rate ATM technology developed by Yurie Systems, Inc., incorporates support for legacy, tactical communications systems, into one piece of equipment, improving operational efficiency. EdgeSpan offers a comprehensive suite of network services. The network services encompasses a broad package of implementation and maintenance features, network management services, and special application support.

EdgeSpan LDR ATM:

- Fully ATM standards compliant
- Seamless integration of legacy communications systems with emerging high-bandwidth applications on a single ATM stream, over facilities ranging from 300 baud to OC-3
    - ATM bandwidth efficiency
    - Integrates multiple transmissions and applications
    - Provides a migration path to ATM, while protecting investment in legacy systems
- Extends ATM operational capabilities to low speed and noisy circuits
- Error correction demonstrated down to 10^{-3} which supports wireless transmission
- Patented traffic management algorithm, AQueMan: Adaptive Queue Management, optimizes voice, data, and video traffic on ATM stream
- Physically designed to operate in deployable environments

AT&T

Government Markets

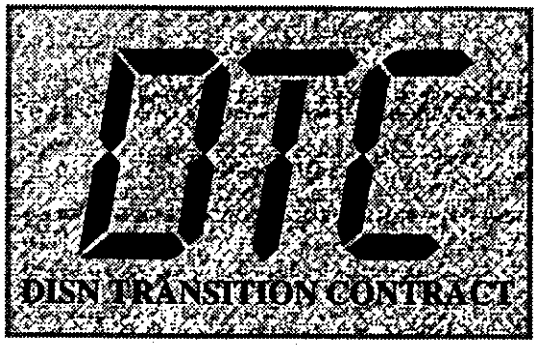
Hawaii Information Transfer System

FACT SHEET

The Hawaii Information Transfer System (HITS) is a contract with DISA to provide information transfer services for encompassing engineering, planning, implementation, and network management including all the functions associated with administration, operation, billing, maintenance and provisioning of a telecommunications network. HITS will provide enhanced capabilities to the Department of Defense (DoD) and certain authorized users on the eight primary islands in Hawaii through a system of seamless and transparent end-to-end switched voice, switched data, Integrated Services Digital Network (ISDN) and dedicated transmission services. HITS also provides interfaces to other DoD networks like DISN, FTS2000, GETS, DSCS and other strategic and tactical networks, and the Public Switched Network.

AT&T

Government Markets



FACT SHEET

The DISN Transition Contract (DTC) was a sole-source award of a new contract to AT&T for the purpose of providing essential telecommunications services in the period after the expiration of the Defense Commercial Telecommunications Network (DCTN) and until the DISN networks are operational, and those services are transitioned.

DTC provides continuity of service for all DoD users, allows for bundling and grooming of services in advance of DISN, assists and advises DISA on transitioning service to DISN, and provides significant savings to DoD during the period of contract performance.

DTC is an end-to-end network and equipment service offering providing all-digital services in support of the Command and Control (C2) requirements of the Department of Defense (DoD). Three primary categories of service are available through the DTC contract:

- Switched Voice
- Switched and dedicated data
- Video Teleconferencing

The DTC provides a wide range of services and capabilities to users, including technical/design support to end-users, a single point of contact for all services, end-to-end responsibility for contracted services, and a dedicated program organization. A full compliment of military-unique features is core to the service to sustain the needs of the warfighter and other support organizations.

Maintenance, administration, and management of the DTC is accomplished through the Dranesville Network Control Center (DNCC) located in suburban Virginia. From this facility AT&T performs centralized control, operations, and maintenance of all DTC systems and sub-systems. The DNCC meets all government criteria for survivability and classified operations.

This network is fully capable of providing critical C3I support to the DoD during military operations and contingencies. DTC network has been a proven and essential element in support of both military operations and business communications within the DoD.

AT&T

Government Markets

FACT SHEET

DISN Video Services - Global (DVS-G) is a reservation-based video service, using bandwidth and switching provided under the DISN Switched/Bandwidth Manager Services - CONUS (BMS-C) and DISN Transmission Services (DTS-C) contracts. The DISN Video community can operate multipoint videoconferences at speeds of 112 Kbps through T1.5 Mbps. Conferences of up to 25 locations can run in either classified (up to Top Secret) or unclassifed mode.

DVS-G serves both dedicated and dial-up video users. Utilizing standards-based bridging equipment, any CODEC that can operate in the standards mode can conference with any other, regardless of manufacturer. Access to FTS-2000 and commercial networks will be provided, as well as bridging for tactical and deployed video applications.

AT&T

Government Markets

FACT SHEET

The DISN Transmission Services - CONUS (DTS-C) contract offers cost effective, reliable, and secure transmission facilities for flexible information transfer capabilities.

The DTS-C contract was awarded to AT&T on January 28th, 1997.

This contract represents:

- Initial SONET connectivity between Bandwidth Manager (BWM) locations at OC-3 transmission rates comprising **Backbone Transmission Services** (transmission capacity to increase over contract life). The SONET backbone will provide high speed, self healing transport connecting 35 bandwidth managers.
- Connectivity between BWM locations and approximately 600 base-level Service Delivery Points (SDPs) at transmission rates ranging from T-1 to T-3 and comprising **Access Transmission Services** (transmission capacity to increase over contract life).
- Network interface equipment:
  existing Government Furnished Equipment will be inventoried, reinstalled and maintained by AT&T,
  new Network Interface Equipment will be provided by AT&T,
  thus, maintaining appropriate interfaces between the DISA end-user locations and transmission facilities at Base Level SDPs.
- AT&T's responsibility for this service terminates at the drop or equipment side of the network interface device.

The intent is for the DTS-C to provide a vehicle for the Government to easily incorporate new technologies, such as ATM, as they become available and deemed beneficial in serving the military community.

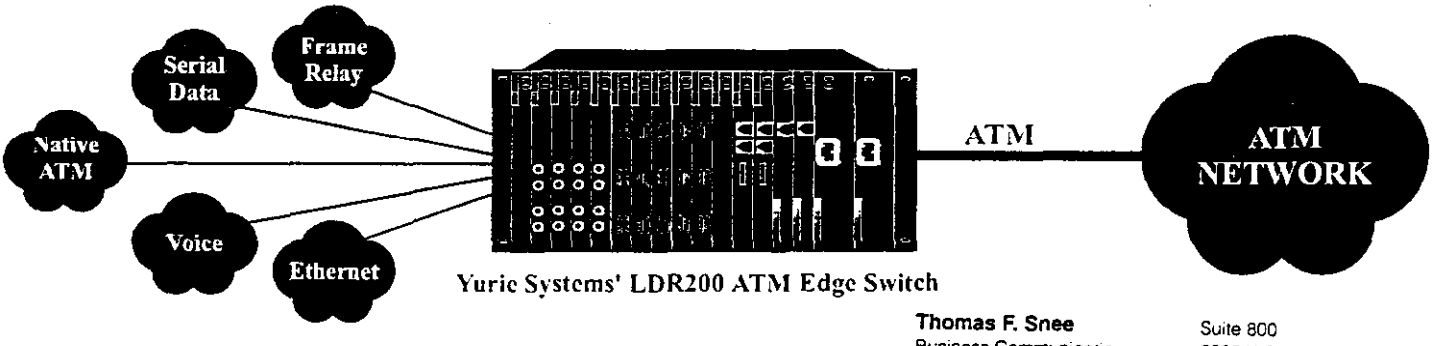
AT&T

Government Markets

EDGESPAN ATM EDGE SWITCH SPECIFICATIONS

SOFTWARE	DESCRIPTION
System Software	Software loaded on CPU Card (1 copy required per shelf)
SNMP Management	SNMP Compliant MIB; Ability to manage vie SNMP Workstation (1 copy required per shelf)
Silence Suppression, Voice	Software to be loaded on DSP 1 Server (1 copy required per DSP 1 card)
ADPCM Voice Compression	Software to be loaded on DSP 1 Server (1 copy required per DSP 1 card)
Encryption	Software to be loaded on DSP 1 Server (1 copy required per DSP 1 card)
ISDN-PRI	Software loaded on DS1 CES I/O Card (1 copy required per shelf)
Frame Relay	Software loaded on DS1 HDLC I/O Card or Multi Serial I/O Card (1 copy required per shelf)
Ethernet, Transparent Bridging	Software to be loaded on DSP 1 Server (1 copy required per DSP 1 card)

SPECIAL FEATURES	DESCRIPTION
ATM Features	ATM Forum 3.0/3.1 PVC, SVC CBR, VBR, UBR Number of VPI/VCI per slot = 32,000 Aqueman adaptive queuing and prioritization (additional traffic management capabilities) Forward error correction on: ATM Header, ATM Payload (per VCI)
Frame Relay Features	FR Forum UNI DTE/DCE LMI: ANSI, CCITT PVC
Interworking Features	FR to ATM service level interworking ISDN PRI to ATM SVC
Network Synchronization	Any I/O port External BITS reference Internal Stratum 3 or 4
Data Security	Virtual circuit-based "key-agile" encryption Industry standard DES algorithm
Error Correction	Forward error correction codes for high-noise applications
Billing Functions	Including cell counting to permit ATM usage-based billing



Yurie Systems' LDR200 ATM Edge Switch

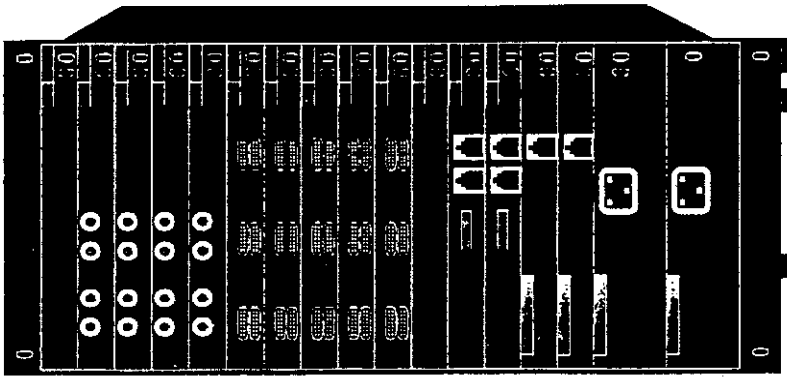
Thomas F. Snee
Business Communications Services -
Defense Markets

Suite 800
2020 K Street, NW
Washington, DC 20006
202 776-6623
RES 301 774-2665
PAGER 800 258-0000
PIN 2880226

Yurie

EDGESPAN ATM EDGE SWITCH SPECIFICATIONS

The Yurie Systems' LDR200 ATM Edge Switch offers a selection of user interfaces to support voice, data, and video applications. A fully configured unit supports 12 interface cards and provides 1.2 Gbps of total bandwidth on the backplane. The switch supports live insertion, enabling any cards to be installed or removed from the unit without the interruption of services on other slots.



PHYSICAL SPECIFICATIONS

DIMENSIONS:

Height: 7"
Width: 19"
Depth: 10.5"
Number of User Slots: 12

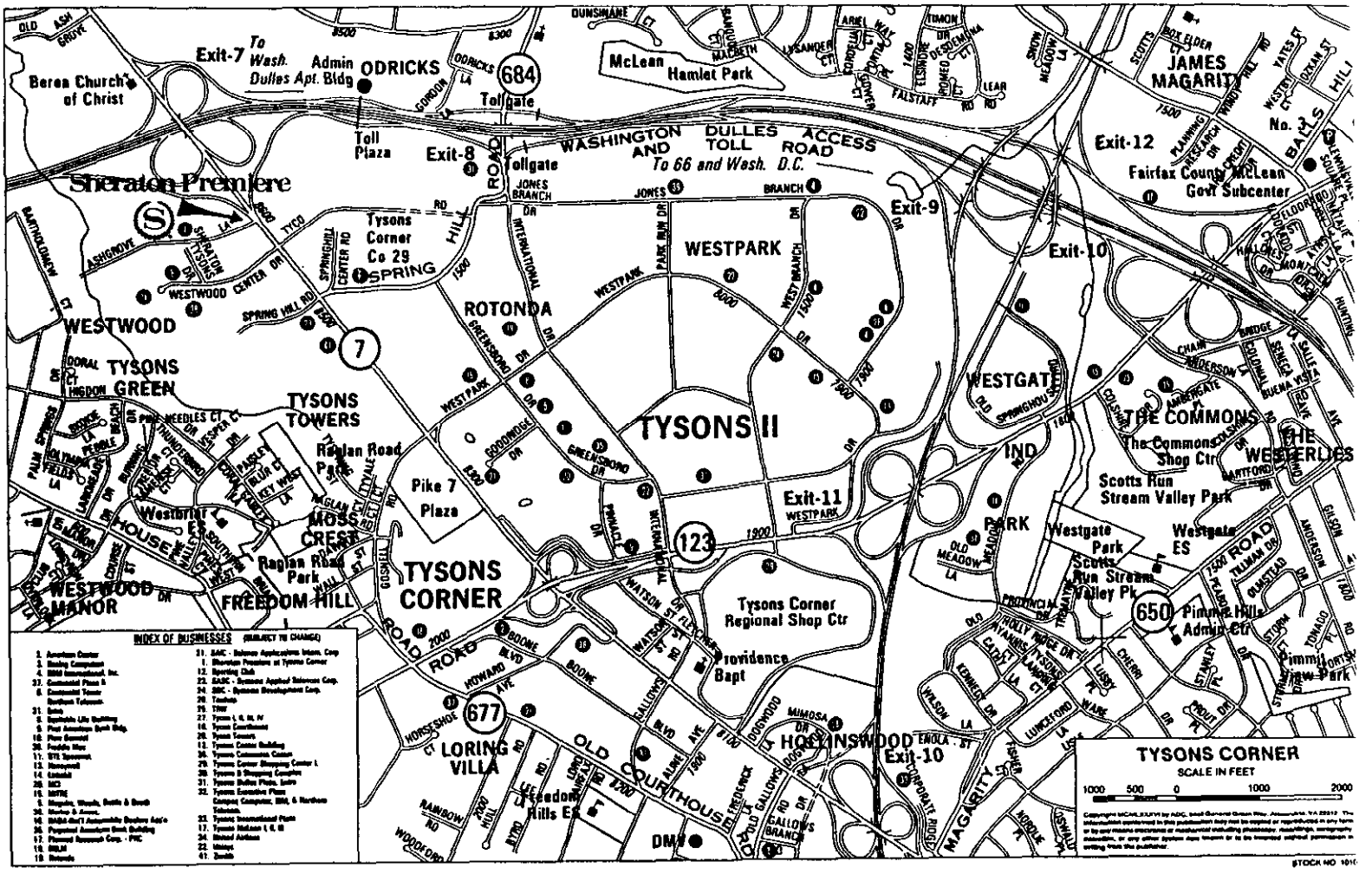
POWER:

Input Voltage: 110/220 VAC
Max consumption: 270 watts
Convection cooling (no fans required)

I/O CIRCUIT BOARDS	DESCRIPTION
Multi Serial I/O	Serial data; Number of ports: 6, Connector Type: micro-DB15; Electrical: RS232, RS422,/449, RS530, V.35; Data Format: Sync, Async; Protocol(s) Supported: ATM, HDLC, FR[1] Terminal Emulation, CES, LANET
DS3 I/O Circuit Pack	Number of Ports: 2; Connector Type: 2 X BNC; Protocol(s) Supported: ATM
DS1 Circuit Emulation I/O Circuit Pack	Channelized T1; Number of Ports: 6; Connector Type: RJ45; Integral CSU; Protocol(s) Supported: CES
DS1 ATM Cell Bearing I/O Circuit Pack	Number of Ports: 5; Connector Type: RJ45; Integral CSU; Protocol(s) Supported: ATM
OC3 LAN Card	Number of Ports: 1; Connector Type: ST Multi-mode Fiber; Protocol(s) Supported: ATM
OC3 WAN Card	Number of Ports: 1; Connector Type: Intermediate Reach Fiber; Protocol(s) Supported: ATM
High Speed I/O	Number of Ports: 2; Port Type: One Serial, One Parallel; Electrical: RS-422, V.35; Line Rate: 50 Mbps per Port; Protocol(s) Supported: ATM LANET
TAXI	Number of Ports: 1; Connector Type: Multi-mode Fiber; Line Rate: 100 Mbps, 140 Mbps; Protocol(s) Supported: ATM
E3 I/O Circuit Pack	Number of Ports: 2; Connector Type: 2X BNC; Protocol(s) Supported: ATM
DSP 1 Server	Required for ADPCM Voice Compression and Silence Suppression. Supports 20 DS0 circuits to be compressed.
2 Wire Source	2 Wire Connection for Station End of Circuit; Number of Ports: 8; Connector Type: RJ11
2 Wire Office	2 Wire Connection for Office or PBX End of Circuit; Number of Ports: 4; Connector Type: RJ11
Enhanced DS1 HDLC I/O Circuit Pack	Channelized T1; Number of Ports: 6; Connector Type: RJ45; Integral CSU; Protocol(s) Supported: HDLC, FR[1]
Ethernet I/O	Number of Ports: 6, Connector Type: RJ45; Protocol(s) Supported: RFC 1483; Transparent Bridging[2]; 6 ports -10 Base T
E1 ATM CES I/O Circuit Pack	Channelized E1; Number of Ports: 6; Connector Type: RJ45; Integral CSU; Protocol(s) Supported: ATM, CES

Yurie

AT&T


Exit-7 To Wash. Dulles Apt.
Admin Bldg
ODRICKS
Toll Plaza
Exit-8
Tollgate
WASHINGTON DULLES ACCESS AND TOLL ROAD
To 66 and Wash. D.C.
Exit-9
Exit-10
Exit-11
Exit-12
Berea Church of Christ
McLean Hamlet Park
Sheraton Premiere
Tysons Corner Ctr 29
SPRING
WESTPARK
ROTONDA
WESTWOOD
TYSONS GREEN
TYSONS TOWERS
TYSONS II
Raglan Road Park
Pike 7 Plaza
MOSS CREST
WESTWOOD MANOR
FREEDOM HILL
TYSONS CORNER
Tysons Corner Regional Shop Ctr
Providence Bapt
LORING VILLA
Freedom Hills ES
HOLLINSWOOD
DMV
WESTGATE
THE COMMONS
The Commons Shop Ctr
THE WESTERLIES
Scotts Run Stream Valley Park
Westgate Park
Westgate ES
Scotts Run Stream Valley Pk
Pimmit Hills Admin Ctr
Pimmit View Park
JAMES MAGARITY
Fairfax County McLean Govt Subcenter
No. 2 Sales
INDEX OF BUSINESSES (SUBJECT TO CHANGE)
TYSONS CORNER
SCALE IN FEET
1000 500 0 1000 2000

DEFENSE INFORMATION SYSTEMS AGENCY
701 S. COURTHOUSE ROAD
ARLINGTON, VIRGINIA 22204-2199

IN REPLY REFER TO: D3 Conference Coordinator
701 S. Courthouse Road
Arlington, VA 22204

March 23, 1997

Dear Conference Attendee:

We have received your registration form and contractor sponsor form (if applicable) for the Annual DII Conference being held 7-9 April 1997 at the Tyson's Corner Sheraton Premiere, 8661 Leesburg Pike, Vienna, Virginia, 22182.

Your registration is confirmed. Enclosed find a conference name badge and a conference admission ticket. As we are expecting a large crowd, it would be advantageous for you to bring your name badge and conference admission ticket to avoid a long wait in line.

A large block of rooms has been reserved at the conference hotel. Please contact them for reservations at 703/448-1234 or fax 703/893-8193.

A map of the hotel area is enclosed for your use.

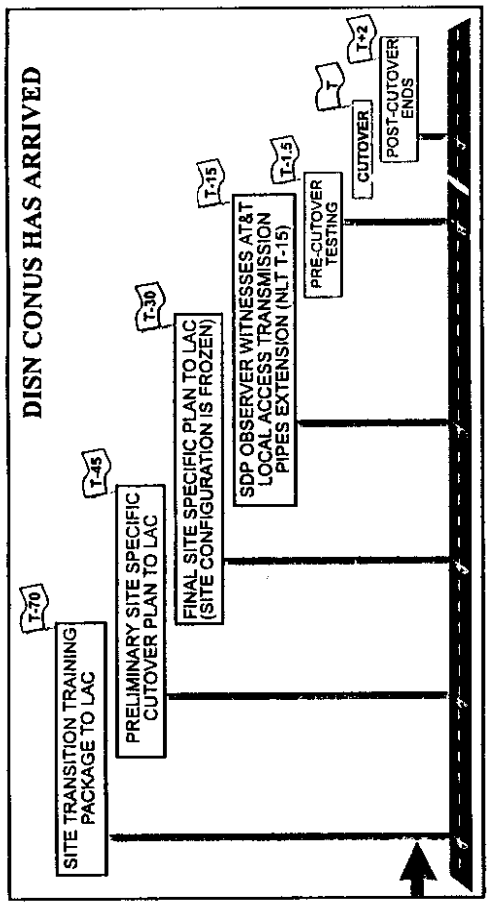
Prior to the conference, you can reach the D3 Conference Coordinator at 703/607-6514 or DSN 327-6514. Conference fax numbers are 703/607-4106 or DSN 327-4106. Conference Email is confered@ncr.disa.mil ('DISA Conference' on the DISA LAN)

We look forward to seeing you at the Annual DII Conference.

D3 Conference Coordinator

DISN GOALS:

- Provide Broadband Services Supporting Mission Needs
- Implement Security Measures to Protect Information Carried on the Network
- Exercise Positive Control of the Telecommunications Infrastructure



DEFENSE INFORMATION SYSTEMS AGENCY (DISA)

DISA is the DOD agency responsible for information technology and is the central manager of the Defense Information Infrastructure (DII). DISA is responsible for planning and supporting C4ISR that serves the National Command Authority (NCA) under all conditions - peace and war. DISA is subject to the direction, authority, guidance, and control of the Assistant Secretary of Defense C3I and is responsible to the Chairman of the Joint Chiefs of Staff for Operational Matters.

DISA MISSION

"To plan, engineer, develop, test, manage, program, acquire, implement, operate, and maintain information systems for C4I and mission support areas under all conditions of peace and war."

DISN CONUS TRANSITION TEAM CONTACTS

Army
- **Major Tim Stark, HQDA**
  DSN 227-0567, Cmcl (703) 697-0567
  Email: starktl@hqda.army.mil

Air Force
- **Capt Thomas Becker, AFCA/SYXM**
  DSN 576-8521, Cmcl (618) 256-8521
  Email: beckert@afca.safb.af.mil

Navy
- **Chief of Naval Operations**
  Major Debra Hall, CNO/N61C21
  DSN 664-7840, Cmcl (703) 604-7840
  Email: hall.debra@hq.navy.mil

Marine Corps
- **Capt Robert de Roziere, USMC/NetOPSCtr**
  DSN 278-2215/3263, Cmcl 784-2215/3263
  Email: deroziere@mqg-smtp3.usmc.mil

Defense Logistics Agency
- **Jim Livengood, CANI**
  DSN 427-3119, Cmcl (703) 767-3119
  Email: james_livengood@hq.dla.mil

All Other
- **Brigette Thomas, DTT**
  DSN 761-6481, Cmcl (703) 681-6481
  Email: thomasb@ncr.disa.mil

DTT URL:
- **http://www.disa.mil/org/mf39.html**
- **DISN Transition Email: disntran@ncr.disa.mil**

DEFENSE INFORMATION SYSTEM NETWORK

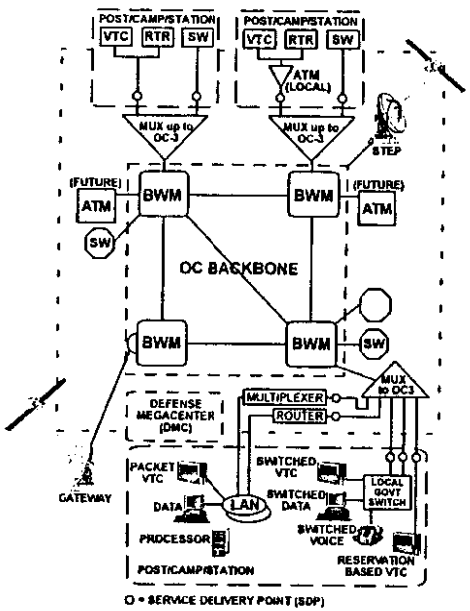
DISN

DISN CONUS TRANSITION

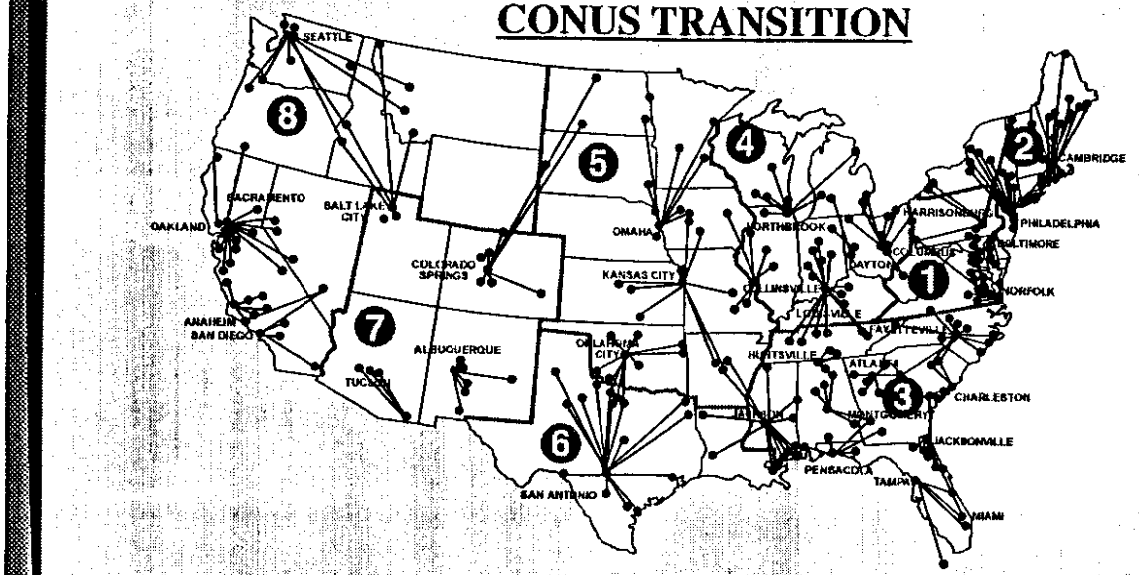
DISN OBJECTIVES:

- Satisfy Warfighter Requirements
- Seamless Connections Between Deployed Forces/Home Bases
- Capitalize on Emerging Technologies
- Interoperable with All DOD Services, Government Agencies, and Allies
- Provide Needed Capacity/Connectivity for Warfighter
- Meet Surge Requirements Anytime/Anywhere
- Rapidly Reconfigurable to Meet Warfighter Needs
- Cost Effective, Affordable Services
- Real-Time Management Capabilities Under All Conditions - Peace and War
- Cost Recovered Through Effective Usage-Based Billing

CONUS CONFIGURATION



CONUS TRANSITION



SERVICE & AGENCY ROLES AND RESPONSIBILITIES

S/A REPRESENTATIVES

- Assist in Transition Planning, Scheduling, Installation Coordination, and Acceptance Planning
- Identify and Coordinate Transition Actions with Local Area Coordinators (LACs) at the Base, Post, Camp and Station Level

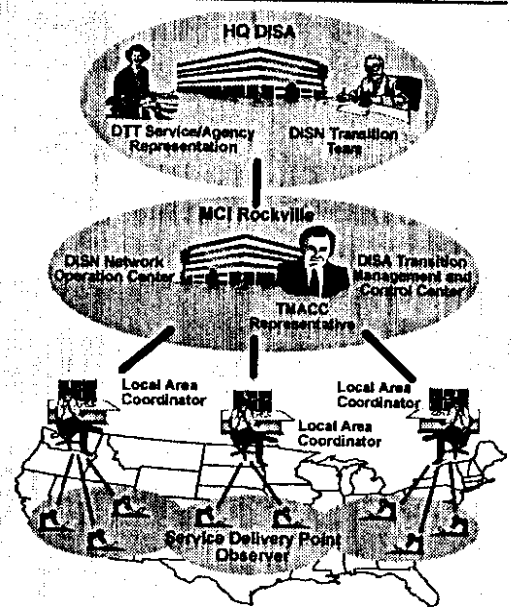
LOCAL AREA COORDINATOR

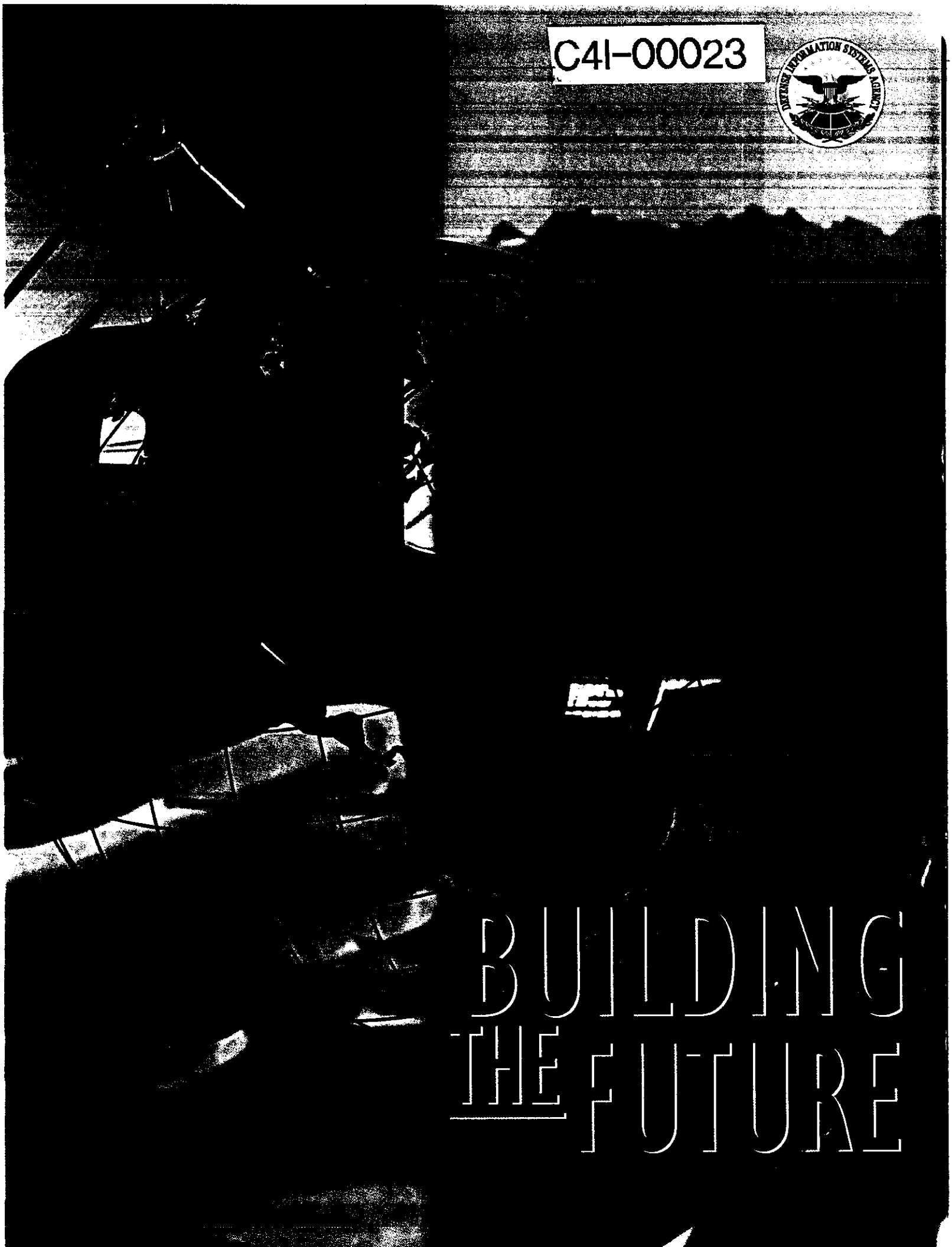
- Provide Local Cutover Assistance
- Review Site Specific Installation Test Plans

SDP OBSERVER

- Provide Service Delivery Point (SDP) Technical Information as Requested
- Record Service Installation and Acceptance Testing
- Submit Implementation Acceptance Test Data to LAC

S/A TRANSITION RELATIONSHIPS





BUILDING THE FUTURE

Joint Interoperability and Engineering Organization (JIEO)

Summary

The mission of JIEO is to ensure interoperability of the Defense Information Infrastructure (DII) and to provide engineering support to warfighters, DISA program and single system managers, Combatant Commands, Services, and Agencies. JIEO provides DOD IS technical architectures and standards, engineers both hardware and software, and supports the acquisition, implementation, development, and integration of secure IS to meet the needs of DOD users in peace and war. JIEO provides interoperable information technology (IT) services and management of IS engineering services to DOD.

Facts/Discussion

JIEO has four centers and four direct reporting units:

--**Center For Standards (CFS),** is the DOD Executive Agent for centralized management of IT standards. The CFS manages the development, adoption, specification, certification, and enforcement of information processing, transfer, and content standards within DOD. CFS also influences the development and adoption by industry of IT standards supporting DOD C4I information systems requirements.

--**Center For Systems Engineering (CFSE),** provides, on a matrix-support basis, design and developmental engineering and RDT&E for all information transfer and network control systems managed by DISA and constituting the information transport for the DII. CFSE provides an engineering facility for the development, evaluation, applications engineering, demonstration, and technology insertion of all transport technologies used within the DII. CFSE provides specialized support to the National Command Authorities (NCA), Joint Staff, Combatant Commands, the Services, and Agencies. CFSE also performs all of the NCA and Nuclear C3 Systems Engineering responsibilities and functions as stated in CJCSI 5119.01 and manages the special program Project Thrift for the Director, DISA.

--**Center For Applications Engineering (CFAE),** develops, maintains, and provides operational support for critical operational systems. Operational systems supported include DISA-internal management information systems, Joint Staff applications, DISA developed and/or maintained Global Command and Control System (GCCS) applications, DISA developed and/or maintained Global Combat Support System (GCSS) applications, and other DOD systems assigned. Meets the software needs of OSD, Joint Staff, DISA (including the Chief Information Office (CIO) and other relevant DISA elements), and other customers as assigned by the Commander, JIEO.

--**Center For Computer Systems Engineering (CFCSE),** implements state-of-the-art software, computer hardware, and data management technologies that provide an efficient, flexible, and secure set of computer systems capabilities that meet the warfighters' requirements. CFCSE engineers the DII, computer systems security, the DII Common Operating Environment (COE) and Shared Data Environment (SHADE), and the Standard Operating Environment (SOE) for the Defense Megacenters (DMCs).

--**DISA Continuity of Operations and Test Facility (DCTF),** provides continuity of operations support to the DMCs and performs integration and testing of GCSS mission applications. The DCTF will support GCSS by building a state-of-the-art prototype model for the DMC of the future. This model facility will then be used to build and test prototype information systems and applications and to implement DII components throughout the DMCs.

--**Operational Support Facility (OSF),** provides C4I and DII life cycle support services such as product integration, technical compliance testing, and configuration management (including metrics collection and analysis of hardware/software and network performance), and systems deployment. The OSF maintains a system integration laboratory and hot line, provides on-site installation and engineering assistance, and assists systems engineers in defining operational requirements for supported systems.

--**DARPA/DISA Joint Program Office (JPO),** the Defense Advance Research Projects Agency/DISA JPO (DDJPO) was established in 1994 by the combined action of the Director of Defense Research and Engineering and the Joint Staff to accelerate the transition of high technology to warfighters in the areas of information systems and information technology, as well as enrich the information services available to DOD users. The DDJPO is making strides in the network arena: a 35-node, wideband asynchronous transfer mode (ATM) network transitioned to the Defense Information System Network (DISN) in FY96 and a Tactical ATM extension was implemented into Bosnia for the Bosnia Command and Control Architecture (BC2A) in support of Operation Joint Endeavor.

--**In Service Engineering Support Facility (ISESF),** provides dedicated CINCs, Services, and Agency support required to plan, engineer, install, train, maintain, sustain, and in some cases operate GCCS platforms to support day-to-day, exercises, special purpose, and contingency mission/operations.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of January 1997)

Joint Requirements Analysis and Integration Directorate (D7)

Summary

D7 is responsible for supporting the functional requirements development, analysis, refinement, validation, and integration across the Department of Defense (DOD). D7 is the sole cross-functional/cross-Service integrator for all functional requirements for the Defense Information Infrastructure (DII).

Facts/Discussion

Using customer-focused teams, D7 assists the functional communities at all levels (Joint Staff, Services, Principal Staff Assistants [PSAs] and Agencies) in the requirements identification and the selection of migrations functionality and near-term strategies for implementing those selections. It assists in the identification and validation of cross-functional and cross-service integration requirements as well as their supportableness in the DII and in supporting segments, such as the Global Command and Control System (GCCS) and the Global Combat Support Systems (GCSS).

Additionally, D7 supports the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD[C3I]) with the implementation of DOD-wide information management programs as they relate to the integration goals and objectives throughout DOD.

D7 has four divisions:

--Joint Staff/Service Combat Support Requirements Analysis and Integration Division, conducts Joint Requirements Analysis and Integration programs in support of the Joint Staff and Military Departments and ensures that combat support and C4I functions are fully integrated with other elements of the DII. Also collects, analyzes, and maintains validated Joint combat support requirements.

--Joint Cross-Functional Program Requirements Analysis and Integration Division, collects and maintains cross-functional requirements and manages cross-functional and cross-Service strategies and plans for migration and integration activities supporting the DII. It also manages migration and integration issues surrounding the DII. Provides migration and integration visibility and program status capabilities. Performs requirements analysis for DISA-led DOD programs and projects.

Defense Information Systems Agency 701 S. Courthouse Road Arlington, VA 22204-2199

--**Finance and Resources Requirements Analysis and Integration Division,** collects and maintains validated functional requirements and identifies, develops and manages cross-functional integration opportunities within Finance, Comptroller and Inspector General functional areas. It also: (a) supports customers in obtaining and managing services under the DEIS and DEIS II contracts, (b) develops and manages DOD's Program Planning, Resource, Contracting, Internal Management Control and Performance Measurement Programs.

--**Acquisition and Technology/Mission Support Requirements Analysis and Integration Division,** collects and maintains validated functional requirements, and identifies, develops and manages cross-functional integration opportunities within the assigned functional areas. It also ensures that Personnel and Readiness functions are fully integrated with other elements of the DII.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of January 1997)

Command, Control, Communications,Computers and Intelligence (C4I) Modeling, Simulation and Assessment Directorate (D8)

Summary

D8 was created in 1994 to provide DISA's Director with sound analytical assessments to support decisions dealing with major DOD and DISA C4I issues. In 1995 the DISA Joint Interoperability Test Center (JITC) was aligned with D8 to consolidate all DISA testing, evaluation, assessment, analysis, and interoperability certification of DOD Joint C4I Systems within a single Directorate.

D8's major activities involve the development of C4I models and simulations that serve as the underpinnings of quantitative analysis and assessment to provide tangible, value-added value support to DOD decision makers such as the Director, DISA; DISA Directorates and program managers; OSD; the Joint Staff; and CINCs, Service and Agencies. The Director, DISA needs the ability to develop a solid, credible and analytical foundation for selecting programmatic options and justifying decisions before top-level OSD officials. D8 was established to address that need and now has achieved demonstratable success in meeting the Director's objectives. Being coupled with JITC's operational testing capabilities gives D8 an enhanced set of assessment capabilities.

D8 is divided into four divisions:

Integration Assessment Division (D81), is a small team of experienced professionals who handle advanced simulation and modeling problems in the areas information processing and design with special emphasis on information warfare. The division specializes in quick response and develops prototype simulation products and methods for examples that resist conventional methods.

CINC Support (D82), provides leading edge C4ISR capabilities to the warfighter communities through the application of modeling, simulation, and assessment technologies. The division examines the ability of the DII/DISN to support the existing war plans in a (Joint) Area of Responsibility or for a special contingency

operation. Assessment expertise is provided to wargames, exercises, and to explore network measurements within the DII/DISN using advanced information MS&A technology. Recommendations for improving the DII/DISN are provided to the appropriate Joint and DISA organizations

Modeling and Simulation (D83), provides M&S support for C4I systems. This support includes developing models that simulate all aspects of C4I and their interactions. Additionally, interfaces are provided that feed the output of Joint models directly to Command and Control systems like GCCS for training and exercise support. The division maintains a database of all DOD information systems and their interfaces. This provides the only tool for performing cross-functional analysis of information flow.

C4I System Assessment (D84), provides decision support to the key DISA programs through leading edge C4I Systems Studies and Analysis. This support includes developing and enhancing the state-of-the-art technology Modeling Simulation and Assessment (MS&A) methods and software tools to support the evolution in DISN/DII. The division also conducts network assessments, "what if" analyses, cost vs. performance trade-off, and optimization studies.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of January 1997)

Western Hemisphere Command (WESTHEM)

Summary

DISA WESTHEM is the largest subordinate command under the Defense Information Systems Agency (DISA) and is responsible for providing information services to all federal agencies in consonance with our primary mission of providing C4I mission support to our nation's warfighters.

WESTHEM was formed as part of the DISA retooling to provide an organizational structure tailored to the primary DISA customers, the warfighters. This familiar structure serves to enhance communication between the service provider and the customer while fostering a strong working relationship in an age of growing information dependency.

Facts/Discussion

DISA WESTHEM is responsible for the operational management of sixteen Defense Megacenters (DMCs) located throughout the Continental United States. Additionally, WESTHEM is responsible for the Joint Staff Support Center (JSSC) located in the Pentagon and the Communication Management and Control Activity (CMCA) located in Sterling, Virginia.

The DMCs, under the framework of the Defense Information Infrastructure (DII), provide end-to-end information services which include information processing, telecommunications and regional information technology support. The DMCs are staffed with a uniquely experienced, dedicated technical personnel and operate 24-hours a day, 365 days a year.

The JSSC, also under the framework of the DII, provides direct command and control information systems support to the Joint Staff. The major elements of DISA WESTHEM include:

--**Center for Combat Support,** manages and directs the operations of the DMCs to include the development and implementation of customer's information service requirements. The Center for Combat Support ensures the delivery of reliable, world-class, competitively priced, information products and services to the Department of Defense and non-defense federal customers.

--**Joint Staff Support Center (JSSC),** responsible for operation, systems maintenance, deployment, and direct customer support of information systems to satisfy the C3 and analytical requirements of the Joint Staff, the National Command Authority (NCA), the Unified Commands, and the Office of the Secretary of Defense (OSD). The JSSC manages and coordinates various administrative and service programs and operations to ensure that total customer requirements are accomplished in a timely, cost effective manner.

--**Communication Management and Control Activity (CMCA),** provides and manages DOD communications support to the U.S. Secret Service (USSS) in the performance of their protective responsibility. Additionally, it provides specialized communications support to law enforcement agencies at the federal, state, and local level for major national and international events approved by Congress and directed by the Secretary of Defense.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of March 1997)

Defense Megacenters (DMCs)

Summary

The Defense Megacenters (DMCs) are automated service facilities responsible for providing information technology support to the Department of Defense (DOD) and non-defense federal customers whose information service requirements are in direct support of the warfighter. There are sixteen operational DMCs located in the Continental United States.

Facts/Discussion

In January 1988, using the Services and Defense Agencies as a basis, DOD embarked on a project to consolidate and subsequently migrate 59 data processing installations (DPIs) into the 16 existing facilities, known as "Megacenters." The data processing workload was transferred from the services and agencies to DISA, in particular DISA WESTHEM, under the Defense Management Report Decision (DMRD) 910 and 918.

Using a drag and drop technique, the DMCs replicated the DPI's processing environments and migrated the automated information systems (AISs) running within these locations to the DMCs. These migrations were successfully accomplished with minimal disruption to the customer while maintaining the same, and often improving, the level of service. Optimization, the final stage of migration, is on-going and will further enhance the operational efficiency of the DMCs and further reduce costs. It is projected that the DOD will save $473.8 million from fiscal years (FY) 1994 to 1999 with this consolidation project.

DMCs operate on a fee-for-service basis. Our original product line was centered around our mainframe processing, but has been expanded to include:

--Mid-tier information processing
--Area comm support (metropolitan area networks)
--Local area network (LAN) support
--Transition client-server support
--Continuity of Operations capabilities (COOP)
--Command and Control Support (GCCS)
--Maintenance
--"First/last-half mile" support to DISN users
--Information services support (PC repair and training)

These additional services are another step toward DISA's vision of providing "end-to-end service" to the warfighter. The DMC concept will allow DISA to effectively/efficiently support warfighter requirements at a regional IT service facility. The DMC enhances system interoperability, while reducing overhead costs by centrally managing multiple operations. This will permit CINCs and Services/Agencies to "outsource" the management of information services to DISA for providing day-to-day information systems support.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of March 1997)

Defense Information Technology Contracting Organization (DITCO)

Summary

DITCO is the procurement arm of DISA which acquires, accounts, and pays for Information Technology (IT) supplies and services required by the Warfighter, Military Departments, DISA, Defense Agencies, and other Federal Agencies.

DITCO supports a worldwide customer base with operating locations in Arlington, VA; Scott AFB, IL; Ft. Shafter, HI; Elmendorf AB, AK; and Sembach AB, Germany. With the exception of the recently consolidated National Capital Region (NCR) office located in Arlington, VA, DITCO operates as a Defense Business Operating Fund-Communications Information Services Activity (DBOF-CISA), using a fee-for-service cost recovery system. The DITCO-NCR office's operational costs are funded by an annual appropriation.

DITCO fulfills customer IT requirements primarily in support of national defense through a full range of procurements. IT services and equipment procured include: telecommunications, networks, systems, point-to-point circuits, equipment and facilities, and special construction as well as computer technology requirements such as: hardware, software, maintenance, and support services.

To accomplish its procurement mission, DITCO employs a world-class, professional workforce spread across ten major functional areas:

--**Command,** responsible to the Director, DISA for the operation of all DITCO activities. Provides direction and guidance and manages the DITCO elements.

--**Mission Support,** plans, develops, implements, operates and manages administrative, facility and military personnel.

--**Office of Civilian Personnel,** develops, establishes, and administers human resource programs for the accession, development, utilization, sustainment and separation of civilian and military personnel.

--**Plans and Procedures,** develops plans and strategies to establish management direction and achieve management objectives. Reviews DISA plans and programs and the commercial IT environment to assess organizational and customer impacts.

Implements and maintains efficient, streamlined procedures, while ensuring compliance with DISA and higher-level directives, regulations and policies.

--**Information Resource Management,** provides life-cycle IT automation and telecommunications support.

--**Information Resources Procurement,** procures commercial IT products and services required for the support of DOD and other Federal Agencies.

--**Comptroller,** responsible for the financial planning, analysis, budgeting, and financial management relative to IT products and services processed through the DBOF-CISA. Provides advice and assistance on all matters relative to telecommunications tariff regulations, rates, and rate structures, for both domestic and international communications services. Provides cost and price analysis as well as negotiation support to DITCO contracting officers throughout the acquisition cycle for all major IT products and services.

--**Legal Counsel**, provides legal service to the DITCO Commander and staff on all legal matters affecting the organization and its procurement operation.

--**Small and Disadvantaged Business Utilization**, supports DITCO customers by promoting socio-economic programs which ensures maximum participation in DITCO acquisitions by all small businesses.

--**Competition Advocate**, promotes the acquisition of commercial items, full and open competition, challenges requirements that are barriers to the acquisition of commercial items.

For more information

Contact DISA Public Affairs at (703) 607-6900.

(As of January 1997)

Electronic Commerce/ Electronic Data Interchange (EC/EDI)

Summary

The main goal of the EC/EDI program is to present a "single-face-to-industry." This means all DOD activities conduct EC using common transaction data standards, a common telecommunications backbone, and a common set of business practices. Objectives of the program are to reduce costs, simplify and speed business transactions, reduce paperwork, decrease inventory, increase transaction reliability and provide a more comprehensive and timely information regarding transaction flow. Each stand alone procurement system within DOD must be migrated to a standard implementation convention and infrastructure.

Facts/Discussion

The Office of the President tasked DOD to take the lead and establish a single EC/EDI infrastructure to support EC across the Federal Government in 1994. A DOD Process Action Team (PAT) was established by the Deputy under Secretary of Defense (Acquisition Reform). This report recommended the implementation of EDI-based contracting systems at 244 DOD installations using a standard-based infrastructure and implementation conventions. The Defense Information Systems Agency (DISA) was tasked with standing up operational capability and the infrastructure was stood up and made operational in mid-1994.

EC/EDI will allow different automated information systems, while using dissimilar technologies, to transmit through diverse communications means to arrive at the final DOD Network, the Electronic Commerce Processing Node (ECPN). Transactions are exchanged via the ECPN between the Government and industry trading partners who subscribe to DOD certified Value Added Networks (VANs).

Currently, the Defense Information Systems Agency (DISA) has established an Electronic Commerce Infrastructure (ECI) with two ECPNs, one at the DISA Defense Megacenter (DMC) Columbus and one at the DISA DMC Ogden, a Central Contractor Registration (CCR), a Standards Management Committee (SMC), a Compliance Certification Facility (CCF) and has assumed Operational Control (OPCON) of nine DOD legacy Gateways.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of March 1997)

Defense Information Systems Agency 701 S. Courthouse Road Arlington, VA 22204-2199

DEIS II

Summary

The DEIS II contracts will provide integration services for the entire Department of Defense (DOD) in support of the Department's migration to an integrated and interoperable Defense Information Infrastructure (DII). More importantly, they will help the Department reach global integration and interoperability by linking the DII to the National Information Infrastructure (NII) and the Global Information Infrastructure (GII). DEIS II will support DISA in facilitating the migration of information systems and common, standard data into the DII, in support of the National Military Strategy and the C4I For The Warrior concept.

DEIS II expands on DEIS by supporting the full development, world-wide deployment, and operations and maintenance management of common, standard, and migration systems. While the original DEIS contracts were used primarily by Defense Agencies and Centers (e.g., DISA, DLA, JLSC, DFAS) DEIS II will be far more useful to the CINCs and Services because of the greatly expanded scope and applicability to support worldwide deployment and sustainment of interoperable and integrated capabilities. The contracts will have a 5-year life cycle ceiling of $2.5 billion for DOD plus $0.5 billion for other Federal Agencies.

Facts/Discussion

DEIS II is a "Best Value" set of awards, based on a "Best Value Assessment and Recommendation." The awardees are **BDM Engineering and Services Co., Boeing Information Services, Inc., Computer Sciences Corporation, EDS, Lockheed Martin Services, Inc., and the Unisys Corporation.**

These companies (all prime contractors on the current DEIS contracts) provide world-class experience and team approaches in a FASA-compliant "Fair Opportunity to be Considered" environment. More importantly, they will help the Department achieve global integration and interoperability objectives. Teams are significantly reconfigured from original DEIS, including the number of subcontractors which ranges from 32 to 48 (vs. 7-18 on DEIS) and 77 percent of the proposed subcontractors are new (i.e., not on current DEIS teams). Of the 245 subcontractors represented on these teams, 142 (58 percent) are Small, Small Disadvantaged, or Woman-Owned Small Businesses or Historically Black Colleges and Universities. Twenty percent of all dollars contracted on DEIS II will go to these Small firms.

All six prime contractors exceed the technical requirements of the RFP and offer prices that compare favorably or are lower than other similar contracts (e.g., original DEIS, INFOSEC, Department of Transportation's "ITOPS") as well as to industry surveys and similar Federal Government labor categories. The majority of labor categories essential to Development, Deployment, and Operations and Maintenance are lower than current DEIS and the DEIS II Independent Government Cost Estimate (IGCE).

"Fair Opportunity" guidance has been prepared and endorsed by the Office of Management and Budget to enable customers to participate in selecting the contractor for a particular requirement while still maintaining appropriate central management control within DISA.

Electronic management tools have been created to allow customers in and outside the Agency online access to current information on how to use the contracts, contractor expertise, deliverables produced, past performance, management metrics, and other factors. Once Statements of Work are awarded these same tools can be used for tracking contractor performance.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of January 1997)

Defense Information System Network (DISN) Switched/Bandwidth Manager Services- CONUS (DS/BMS-C)

Summary

MCI Telecommunications Corporation has been awarded Contract DCA200-96-D-0096 for Defense Information System Network (DISN) Switched/Bandwidth Manager Services - CONUS (DS/BMS-C). **It is a fixed price, indefinite delivery/indefinite quantity (IDIQ) contract with a three-year base period and six one-year renewal options.**

Facts/Discussion

The DS/BMS-C will provide within the continental United States (CONUS) the switched circuit/voice and bandwidth manager service elements of the DISN. The DISN will allow warfighters to "reach back" and use the capabilities of the Defense Information Infrastructure (DII) from any deployed location as well as supporting daily Department operational requirements.

The purpose of the DS/BMS-C contract is to provide and manage transmission bandwidth managers at selected locations within CONUS that form the long-haul backbone of the DISN transport layer. These nodal points will concentrate information from within its serviced access area and transmit that information over the DISN CONUS SONET-based backbone to its terminating node. Both the SONET-based backbone and access area transmission services are being provided through a separate solicitation. Additionally, the DS/BMS-C contract will provide within CONUS the tandem circuit switch backbone element of the Defense Switched Network, the Department's command and control voice communications service.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of January 1997)

Defense Information System Network (DISN) Transmission Services - CONUS

Summary

AT&T Government Markets has been awarded Contract DCA200-97-D-0048 for Defense Information System Network (DISN) Transmission Services - Continental United States (CONUS). It is an Indefinite Delivery/Indefinite Quantity (IDIQ) contract with a ceiling price of $5,000,000,000. The contract life is for a one year base period with eight one year options.

Facts/Discussion

AT&T, in response to Delivery Orders issued under the DTS - C contract, will provide wideband fiber based transmission bandwidth for a DISN CONUS Synchronous Optical Network (SONET) backbone and wideband, generally fiber based, transmission bandwidth connectivity to user locations at approximately 600 DOD user locations in CONUS. The SONET backbone will employ optical fiber and provide information transport between the DISN Bandwidth Managers acquired under the DISN Switched/Bandwidth Manager Services - CONUS contract.

For the access areas, AT&T will provide information transport for the aggregate bandwidth of all customer Service Delivery Points homed off the Bandwidth Managers located in their respective access areas. To take advantage of the bulk transmission rates, AT&T will bundle the access transmission into SONET for delivery to the Bandwidth Managers. At the customer access locations, transmission bandwidth interfaces at T1, T3 and SONET will be provided. AT&T will team with Local Access Providers as required to accomplish the access area bandwidth requirements.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of February 1997)

Defense Information System Network (DISN) Video-Services - Global

Summary

AT&T Government Markets has been awarded Contract DCA200-97-D-0054 for Defense Information System Network (DISN) Video Services - Global. It is a Fixed Price Indefinite Delivery/Indefinite Quantity (IDIQ) contract with a ceiling price of $125,000,000. The contract is for a three year multi-year base period with two one year options.

Facts/Discussion

The work will be performed at Department of Defense (DOD) locations worldwide. The contractor will provide multi-vendor interoperability, dedicated video services including secure and non-secure, point-to-point and multi-point bridging, a reservation/scheduling system, video services management and monitoring, provisioning and user-site network interface equipment.

This award includes the final CONUS piece of a multi-contract acquisition strategy. The DISN Acquisition Strategy consists of short term, competitively awarded contracts that will provide DISA with substantially increased control over costs and network management. It will ensure positive control of the global DISN, foster greater competition, integrate commercial products, and help the government reduce the cost of satisfying communications and video teleconferencing requirements of the warfighters.

The DISN Video Services Contract will greatly enhance DOD's ability to provide video teleconferencing services to meet the requirements of the warfighters.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of March 1997)

Defense Information System Network (DISN) Support Services-Global (DSS-G)

Summary

Boeing Information Services, Inc. has been awarded Contract DCA200-96-D-0065 for Defense Information System Network (DISN) Support Services - Global (DSS-G). It is a one-year time-and- materials, indefinite delivery/indefinite quantity (IDIQ) contract with four one-year renewal options.

Facts/Discussion

The DSS-G will serve as the technical management support vehicle for the DISN. This network will allow warfighters to "reach back" and use the capabilities of the Defense Information Infrastructure (DII) from any deployed location.

The purpose of the DSS-G contract is to support DISA's life-cycle management of the DISN with world-wide support services. These support services include, but are not limited to: program management support; engineering services; integrated logistics support (ILS) planning; service provisioning support; network management support; hardware and software maintenance; subscriber integration services; management information system (MIS) support; and training. The Department of Defense (DOD), its Agencies, the Military Services and other Federal Government Departments may acquire support services under this contract via task orders through DISA.

A Task Order Guide is available for information and use through Mr. Michael Buehler, DISA. Please call (703) 681-5432 or DSN 761-5432 for agencies interested in placing a task order under this contract.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of January 1997)

DEFENSE INFORMATION SYSTEMS AGENCY
701 S. COURTHOUSE ROAD
ARLINGTON, VIRGINIA 22204-2199

IN REPLY REFER TO: Operations (D3)

APR 0 1 1997

MEMORANDUM FOR CONFEREES AT THE ANNUAL DEFENSE INFORMATION INFRASTRUCTURE CONFERENCE

SUBJECT: Conference Welcome

1. Welcome to the Defense Information Infrastructure Conference. You will notice that we have combined many Defense Information Systems Agency (DISA) forums normally held throughout the year into this one major conference. We believe this will maximize your time and travel dollars and will also effectively demonstrate the critical relationships between core programs. This will, however, require you to make decisions as to which ones are most applicable to your interests.

2. I do hope that you will take some time during the 3 days of the conference to visit the demonstration area. You will see examples of many exciting C4I projects that are underway which will provide a visual glimpse of the future.

3. As many of you know, I will be retiring in June after 3 years as DISA's Director. It has been a professionally satisfying tour, and I appreciate the successful working relationships. Through our combined government-vendor team, much has been accomplished to prepare our forces for the 21st century. However, there is still more work to do. We must continue to bring our best professional workforce together to complete these critical issues.

4. I encourage you to maximize your attendance this week through open participation and then to share your newfound knowledge with coworkers when you return to your office. I look forward to hearing your ideas and comments.

ALBERT J. EDMONDS
Lieutenant General, USAF
Director

ADMINISTRATIVE REMARKS
DISA ANNUAL DEFENSE INFORMATION INFRASTRUCTURE CONFERENCE

Welcome to DISA's Annual Defense Information Infrastructure (DII) Conference. Thank you for taking the time to attend this year's conference. We trust you will find the information and discussions useful.

For your convenience, this information sheet contains administrative remarks to help while you are at the conference. If we can answer any further questions, please do not hesitate to ask one of the conference staff wearing beige badges. From 0700 to 1800, you can always find a staff member in the Conference Operations Center.

OPERATIONS CENTER. The Operations Center will be able to take telephone messages for you and post them on the message board. You should instruct those who need to contact you to call (703) 873-9597/8. Incoming faxes (please keep them short) can be sent to (703) 873-9596. There is a small photocopier which can make limited numbers of copies. The Operations Center can assist you if you need a new name badge, conference information, or directions to a subconference room. A small number of cell phones will be available in the Operations Center for designated personnel.

PUBLIC TELEPHONES. The hotel provides a bank of telephones for outgoing calls. The telephones are located on the lobby level. These phones are plentiful and available for all conference participants.

ADMITTANCE TICKET. If you have not already done so, please deposit your admittance ticket in one of the boxes by the entry to the main conference room. These tickets help us keep track of attendance, as well as record the representation from various agencies and commands.

SIGN UP SHEETS FOR SUB-CONFERENCES. Be sure to sign up quickly for the afternoon subconferences. Multiple conferences will be conducted at once and we need to know the numbers of people planning to attend so we can ensure the room sizes are adequate. Sign up sheets are located near the Conference Registration Desk. For subconferences on 7 April, it is especially important that you sign up early. Room assignments for afternoon subconferences may be adjusted based on the number of people signed up by 1100 on 7 April. We suggest that on Sunday evening or Monday morning

you also sign up for the subconferences on the following days. Sign up sheets for all subconferences will remain posted until 1100 on the day of the subconference.

BRIEFER SUPPORT. If you are presenting a brief during the General Session, please check in with Major Rich Earl, USMC. Major Earl will assist you with electronic projection of your brief and ensure you have a microphone. Major Earl will be in the Grand Ballroom or at the Operations Center. You can ask any conference staff member to help you find him.

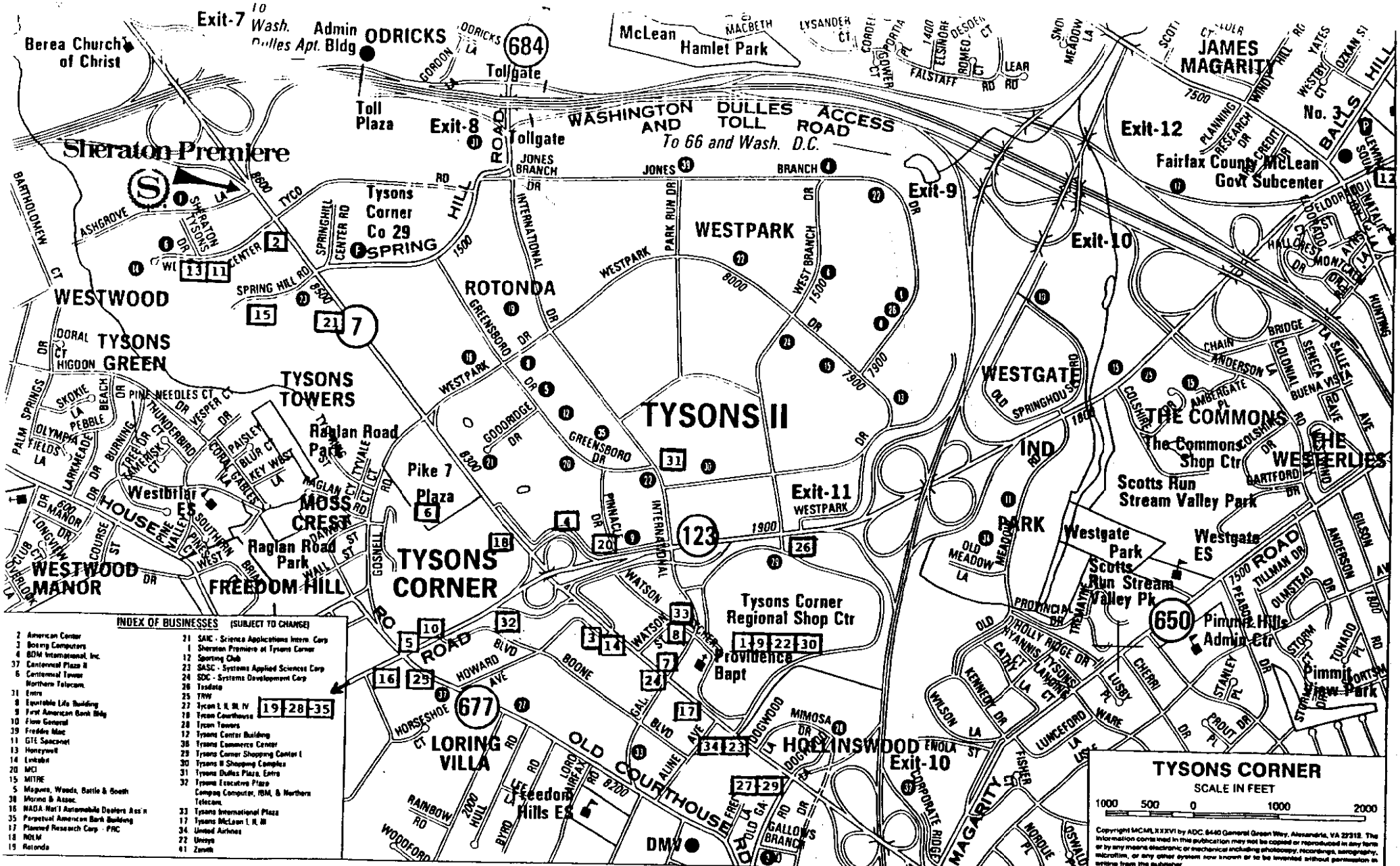
DEMONSTRATIONS. A number of demonstrations are available in the Junior Ballroom. This area is small but we will have it open a half hour before the conference begins each day, and then again from the lunch break throughout the afternoon.

COPIES OF BRIEFS. Copies of the General Session briefs will not be available prior to the conference. This decision was made to preserve resources as well as to ease the weight of your luggage on your trip home. When you return to your commands, you may download copies of the main session briefs from the DISA web site. It is our intent to post the briefs on the web site by 18 April 1997. Copies of subconference briefings can be obtained directly from subconference POCs.

FOOD AND BEVERAGE. As a convenience to you, and since there is no conference fee, there are multiple locations to purchase food and beverage. The Sheraton will provide food carts in the morning and during scheduled breaks. These carts will be by the Grand Ballroom so you may purchase coffee, snacks, and sandwiches. The hotel will try this on Monday, 7 April, and if there is enough interest, the hotel will have the carts available each of the three conference days. Full meals are served in the hotel restaurants and at nearby facilities. There is a separate sheet in your folders listing nearby restaurants. Our conference schedule provides 90 minutes each day for a lunch break.

THIS IS AN UNCLASSIFIED CONFERENCE. No portion of this conference will be held at a classified level. Please keep your comments and questions unclassified.

			PHONE #	ADDRESS
	AshGrove's	**Fine Dining**	**Ext. 7042**	**Sheraton Premiere**
		American	**Ext. 7066**	**Sheraton Premiere**
1	America	American	847-6607	Tyson's Corner Mall
2	American Cafe	American	848-9476	8601 Westwood Cente
3	Benningan's	American	556-9417	8219 Leesburg Pike
4	Clyde's	American	734-1900	8332 Leesburg Pike
5	Friday's	American	556-6173	2070 Chain Bridge Rd.
6	Mr. Smith's of Georgetown	American	893-5500	8369 Leesburg Pike
7	Mustache Cafe	American	893-1100	8250 Leesburg Pike
8	Silver Diner	American	821-5666	8101 Fletcher St.
9	Slade American Grill	American	760-9030	Tyson's Corner Mall
10	Hunan Lion	Chinese	734-9828	2070 Chain Bridge Rd.
11	The Oriental Regency	Chinese	827-9066	8605 Westwood Center Dr.
12	Evan's Farm Inn	Country	356-8000	1696 Chain Bridge Rd.
13	Ring Master Deli	Deli	448-4444	8607 Westwood Center Dr.
14	Boston Market Chicken	Fast food	917-7979	8221 Leesburg Pike
15	Fuddrucker's	Fast food	821-8581	1587 Spring Hill Rd.
16	Mc Donald's	Fast food	393-9489	2089 Chain Bridge Rd.
17	Roy Roger's	Fast food	[illegible]-4996	8022 Leesburg Pike
18	Wendy's	Fast food	[illegible]025	8353 Leesburg Pike
19	Bonaroti	Italian	281-[illegible]0	428 E. Maple Av.
20	Da Dominico	Italian	790-900[illegible]	1992 Chain Bridge Rd.
21	Fedora Cafe	Italian	556-0100	[illegible]21 Leesburg Pike
22	Lucieno	Italian	893-8488	Ty[illegible]n's Corner Mall
23	Primi Piatti	Italian	893-0300	804[illegible] Leesburg Pike
24	The Olive Garden	Italian	893-3175	8133 [illegible]esburg Pike
25	Narita	Japanese	893-8008	8417 O[illegible] Court House Rd.
26	Chi-Chi's	Mexican	893-2443	1951 Chai[illegible] Bridge Rd.
27	Chili's	Mexican	734-9512	805[illegible]esb[illegible]g Pike
28	Anita's	New Mexican	255-1001	521 E. Maple Av.
29	Bertucci's	Pizzeria	893-5200	8027 Leesburg Pike
30	California Pizza Kitchen	Pizzeria	761-1773	Tyson's Corner Mall
31	Legal Sea Food	Sea Food	827-8900	Tyson's II (Galleria)
32	Phillip's Sea Food	Sea Food	442-0400	8330 Boone Blvd
33	JR's Stockyards Inn	Steakhouse	893-3390	8130 Watson St.
34	Morton's of Chicago	Steakhouse	883-0800	8075 Leesburg Pike
35	Outback Steakhouse	Steakhouse	242-0460	315 E. Maple Av.



STOCK NO. 10106

DII DEMONSTRATIONS

Junior Ballrooms

Demo & (Time)*	***Description***
GCCS/GCSS (Continuous)	Demonstration of the GCCS and GCSS capabilities that support C4I warfighter.
DMS (Continuous)	Demonstration of the functionality of Microsoft, Lotus and Enterprise Solutions Limited messaging applications.
DISN Transition Team (DTT) (Continuous)	Provides an executive overview slide show of the DTT efforts including status of contracts and latest schedule.
Information Assurance/INFOSEC Training and Awareness (Continuous)	Following videos and CDS will be available for viewing. "Networks at Risk" "INFOSEC Awareness" "Protect Your AIS" "Information Front Line" "Bringing Down The House" "Secure Products Database" "Training Resources Electronic Catalog"
Information Assurance Tools (Continuous)	Demonstration of network detection and intrusion tools such as Viper and NID. A simulated network attack will be shown.
DISN Modeling (1:30pm)	Demonstration of the modeling and analysis of DISN, using NetMaker, in support of OT&E.
DMS Messaging Model (2:00pm)	Demonstration of the DMS Messaging Model to support system engineering, deployment and implementation of DMS.
DMS Performance Modeling Using BEST/1 (2:30pm)	BEST/1 is a computer performance assessment and modeling tool used for performance analysis and modeling of DMS component computing platforms.
DMS User Process Modeling and Benefits Analysis (3:00pm)	Demonstration will discuss the writer-to-reader benefits of DMS to organizational and individual messaging users.

DISA/JIEO Center for Computer and Systems Engineering (CFCSE) DII Data Dictionary Tools (Continuous)	Two DII Data Dictionary Tools will be demonstrated. The first tool, a Data Dictionary Repository System, demonstrates an Oracle forms interface used to store and maintain standard metadata about information used by all DoD agencies. The second data dictionary tool, a Personal Computer Data Access Tool is designed for a stand alone system using a CD-ROM.
Software Enterprise License (SEL) (Continuous)	Demonstration of information available on the different SEL web sites, including DISA's, the SPO's, and Logicon's, and to show the interaction between these sites.
Reference Data Sets (Continuous)	Demonstration of the web page that is used to share over 60 standard reference data sets (e.g., country code, supply class, transportation mission) with the DOD community.
Scenario Assessment Model (SAM) (Continuous)	Demonstration of current effort to support the warfighting CINCs, JCS, ASD(C3I), and DISA by identifying deficiencies and opportunities within existing and proposed communication architectures through the use of modeling and simulation.
Trouble Management System (TMS) (1:00pm & 3:00pm)	Demonstration of the standard DII Control Center tool (Remedy) used to initiate and transfer trouble ticket information.
Integrated Network Management System (INMS) (1:00pm & 3:00pm)	Demonstration of the ability to monitor and actively manage diverse networks from one multifunction workstation.
Configuration Management (CM) (1:00pm & 3:00pm)	Demonstration will show a capability of displaying a physical layout and location of equipment within a network management center down to rack level and query the database for cross connects and equipment. The ability to query an IP database for networks, subnets, and equipment will also be demonstrated.

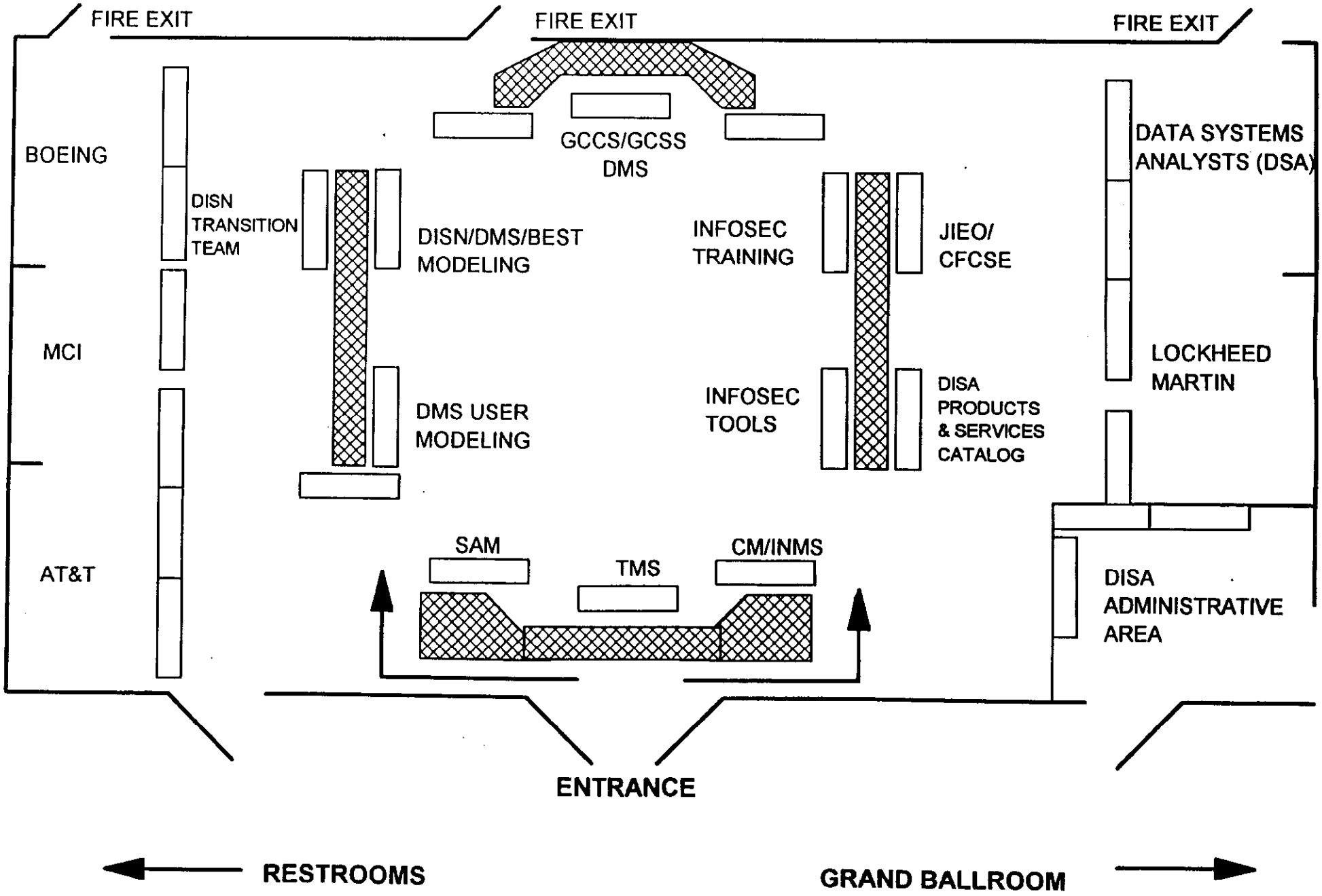
DISA Products & Services Information Catalog (Continuous)	Demonstration of access to a Web page to review products and services provided by DISA.
Data Systems Analysts, Inc. (DSA) (Continuous)	Provides displays in support of the DMS program office. -A "document tree" which shows relevant documentation in support of DMS. -Electronic Mail Address Directory and Registration Process. -Functional, Security, and Performance (FSP) Testing. -Network and Topology Design of DMS. -Support provided during transition from AUTODIN to DMS.
AT&T (Continuous)	Static display highlighting the Hawaii Information Transfer System (HITS), DISN Video Services-Global (DVS-G) and DISN Transmission Services - CONUS contracts. A Yuri 200 Limitless Data Rate ATM Switch will also be present.
MCI (Continuous)	Provides information on the DISN Switched/Bandwidth Manager Services - CONUS (DS/BMS-C) contract.
Boeing (Continuous)	Boeing representatives will be present to discuss their role in the DISN Support Services - Global (DSS-G) contract as well as the support they provide through DEIS and other contracts.
Lockheed Martin (Continuous)	Demonstration of the DMS Infrastructure Components and User Agents (Microsoft, ESL and Lotus) and Interoperability with others electronic mail user agents and components.

*DISA booths will be staffed from 0700 until start of conference each day and will be closed during the general briefing sessions.

All booths will be open from 11:30am - 5:30pm.

Some demonstrations are scheduled at specific times which are indicated. However, these booths will still be staffed at all other times and additional demonstrations can be presented upon request.

DEFENSE INFORMATION INFRASTRUCTURE DEMONSTRATIONS



The Defense Information Systems Agency (DISA)

The Defense Information Systems Agency (DISA) is a Department of Defense (DOD) combat support agency under the direction, authority and control of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD[C3I]). It is the central manager of major portions of the Defense Information Infrastructure (DII). The DII will integrate critical warfighter mission and logistic support into a single infosphere that is interoperable and secure.

The Agency began in 1960 as the Defense Communications Agency (DCA), with the goal of consolidating the communications functions that were common to the military departments. The name changed to DISA in 1991 to better reflect its role in providing total information systems support. The Agency is responsible for providing a seamless web of communications networks, computers, software, databases, applications and other capabilities that meets the information processing and transport needs of DOD users in peace and all crises, conflict, humanitarian support and wartime roles.

DISA's main objective is to anticipate and respond to the needs of its customers, the warfighters, by providing them with seamless, end-to-end, innovative and integrated information services which provide a fused picture of the battlefield. It is responsible for planning, developing and supporting command, control, communications, computers and intelligence (C4I) and information systems that serve the needs of the National Command Authorities (NCA) under all conditions of peace and war. It provides guidance and support on technical and operational C3 and information systems issues and coordinates DOD planning and policy for the integration of C4I systems and the insertion of C4I for the Warrior (C4IFTW) leading edge technologies into the DII.

DISA ensures the interoperability and integration of C4I systems such as the Global Command and Control System (GCCS), Global Combat Support System (GCSS), Defense Information System Network (DISN), Defense Message System (DMS), theater and tactical command and control systems, Allied C4 systems and those national and international commercial systems that affect the DISA mission. It also manages the Defense Megacenters (DMCs) and supports the national security emergency preparedness telecommunications functions of the National Communications System (NCS).

DISA will provide support to the warfighters regardless of where they are located, what their mission or what uniformed service or allied nation they belong. It is important that DISA be recognized as the sole provider for the Nation's warfighters in terms of reliable, flexible and affordable information systems support.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of March 1997)

Defense Information Systems Agency 701 S. Courthouse Road Arlington, VA 22204-2199

Defense Information Infrastructure (DII)

Summary

The DII is the seamless web of communication networks, computers, software, databases, applications, data, security services, and other capabilities that meet the information processing and transport needs of DOD users in peace and in all crises, conflicts, humanitarian support, and wartime roles. It implements the C4I For The Warrior (C4IFTW) vision of an user-driven infrastructure through which warfighters and other DOD users can quickly share needed information from any location, at any time using secure voice, text, and video services. The DII will allow warfighters to see a fused, real-time, true representation of the three dimensional battlespace.

Facts/Discussion

The DII will allow U.S. Forces to meet the needs of the National Military Strategy: U.S. Forces must be able to project power from Continental U.S. bases, sanctuaries and in-theater locations in times of conflict, plus support up-to-the-minute peacetime missions.

The DII will operate as a collection of distributed, heterogeneous information systems. It will range from DOD applications implemented at central locations, to base-level or end-user applications on desktops or in tactical environments. The infrastructure requires collaborative development reflective of its cooperative ownership among the Office of the Secretary of Defense (OSD), the Joint Staff and individual services and agencies.

The current DII consists of many elements, much like a puzzle in which each piece is crucial to the overall picture. These elements build on and include a foundation of integration and technology support. It is important that the DII evolve to support new and existing missions, to provide new capabilities, and to introduce new technology.

The DII includes:
--the physical facilities used to collect, distribute, store, process, and display voice, data, and imagery.
--the applications and data engineering practices (tools, methods, and processes) to build and maintain the software that allow C2, intelligence, surveillance, reconnaissance, and mission support users to access, manipulate, organize, and digest proliferating quantities of information.

--the standards and protocols that facilitate interconnection and interoperation among networks and systems and provide security for the information carried.
--the people and assets which provide the integrating design, management and operation of the DII, develop the applications and services, construct the facilities, and train others in DII capabilities and use.

The Defense Information Systems Agency (DISA) works with the CINCs, Services and other Agencies to develop the DII Master Plan for ASD(C3I). The DII Master Plan is a living document that establishes the common DOD vision for the DII, identifies current and future elements, defines DII participants' roles, responsibilities and relationships, and identifies the relationships and interdependencies of key initiatives.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of January 1997)

Global Command and Control System (GCCS)

Summary

The C4I for the Warrior (C4IFTW) concept is committed to the challenge of meeting the warrior's quest for information needed to achieve victory for any mission, at any time, and at any place. C4IFTW is the vision and roadmap for creating a broadly connected joint system providing total battlespace information to the warrior.

Joint operations involving multiple land, sea and air units in adaptive joint force structures increasingly require joint networks and joint systems that are fully interoperable horizontally across air, sea, space and ground environments. This is the ultimate goal of C4IFTW. The Global Command and Control System (GCCS) is the midterm solution and the bridge to the concepts outlined in the C4IFTW concept. GCCS is C4IFTW in action, today.

Facts/Discussion

GCCS is a common operating environment (COE), integration standard, and migration strategy that eliminates the need for inflexible stovepipe command and control systems and expensive duplication. It is the migration of existing systems into a new COE connected across the Secret Internet Protocol Router Network (SIPRNET) and the integration of selected command and control (C2) systems into a comprehensive, interoperable system.

Its first priority is to demonstrate the C4IFTW concept's vision by becoming a globally connected, warrior-involved, interoperable, fully-integrated C4 system. The GCCS core consists of the basic functions required by the warfighter to plan, execute, and manage military operations. These functions are then satisfied by selecting the applications from existing C2 systems that best meet the requirement. This ensures interoperability, minimizes training requirements and allows efficient use of limited defense resources. GCCS has been identified by the Assistant Secretary of Defense for Command, Control, Communications and Intelligence as the C2 migration system to meet the goal of migrating the many Service systems into fewer, better integrated systems.

Defense Information Systems Agency 701 S. Courthouse Road Arlington, VA 22204-2199

GCCS is not a traditional acquisition program nor a grand design effort that is difficult or cumbersome. It remains simple and straightforward, being implemented one step at a time as user feedback helps build the next step. It implements a flexible and highly adaptive client-user architecture, tailored for the warfighter as specified by the warfighter.

On August 30, 1996, DISA officially pulled the plug on the Worldwide Military Command and Control System (WWMCCS) Intercomputer Network (WIN). Concurrently, the Joint Staff declared the Global Command and Control System (GCCS) as the joint command and control system of record.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of January 1997)

Global Combat Support System (GCSS)

Summary

The C4I for the Warrior (C4IFTW) concept is committed to meet the warrior's information requirement to achieve victory for any mission, at any time, and at any place. C4IFTW is the vision and roadmap for creating an integrated combat support picture for the warfighter.

GCSS is the final piece of the C4IFTW concept. It is a demand-driven, joint warfighter-focused initiative to accelerate delivery of improved combat support capabilities. Using the same approach, methodology, practices, tools, and integration procedures as the Global Command and Control System (GCCS), GCSS is a *strategy* that integrates existing combat support systems to gain efficiency and interoperability in support of the warfighter. GCSS will provide the warfighter with a fused, real-time combat support view of the battlespace.

Facts/Discussion

Currently, the Joint Task Force has stovepiped information systems in logistics, engineering, finance, acquisition, and health services. GCSS will eliminate these stovepipe systems and develop shared information database access via a single computer.

One of the components of GCSS is the Electronic Commerce (EC)/Electronic Data Interchange (EDI) infrastructure initiative. This initiative enables the warfighter to electronically access goods and services in a timely and efficient manner via the Electronic Commerce Infrastructure (ECI).

GCSS will create a technical environment and process to economically integrate existing computer-based systems software and hardware using the common operating environment (COE) and shared data environment (SHADE). It will also expand the GCCS COE to accommodate combat support applications and will also provide "split base-reachback" capabilities from the foxhole to the sustaining base to allow the warfighter to be "deployed" by electronic means.

GCSS provides on-line connectivity to NIPRNET/SIPRNET web and access to applications and data. GCSS will have heavy user participation, and through incremental improvement will evolve to hardware independence and interoperability.

GCSS goals are to:

--Provide reachback to combat support capabilities and personnel that remain in garrison.
--Provide a combat support infrastructure that is responsive to mission support needs.
--Provide a flexible and adaptive open computing environment.
--Enable interoperability and integration across combat support areas and from combat support to the combat environments.
--Integrate and implement an information infrastructure that provides end-to-end information connectivity and access.

GCCS and GCSS both need the Defense Information System Network (DISN) and the Defense Message System (DMS) to complete C4IFTW. GCSS will rely on all components of the DISN for information transport services including voice, text, and imagery. DMS provides the warfighter a secure, reliable, and accountable writer-to-reader messaging infrastructure at reduced cost.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of March 1997)

Defense Information System Network (DISN)

Summary

The Defense Information System Network (DISN) comprises the DOD consolidated worldwide enterprise-level telecommunications infrastructure which provides the end-to-end information transport for supporting military operations, national defense C3I requirements, and corporate defense requirements. DISN provides the primary transmission path to support the Defense Information Infrastructure (DII). DISN features a backbone capability in CONUS with Synchronous Optical Network (SONET) transmission. This transmission is integrated with military and commercial leased communication satellites, switched voice and data services, SONET bandwidth managers, and teleconferencing services.

Facts/Discussion

In July 1995, DISA announced its strategy for the next generation global telecommunications infrastructure that would support the Nation's Warfighters worldwide. As a result, DISN would replace expiring contracts and aging systems with a global approach designed to take maximum advantage of industry capabilities and evolving technologies. The goal architecture represented a graceful technological evolution from the use of DOD-owned and operated networks and systems to commodity services where possible.

The DISN strategy will consolidate more than 100 independent DOD networks into a single, integrated, cost effective, efficient, common-user global "infosphere," a grid that will provide connectivity on demand anytime, anywhere. This will help alleviate the problem with individual legacy communications systems which are not effectively integrated and often non-interoperable. Today, these disparate systems impede or even prevent the exchange of information between warfighting commands and units. DISN serves as the evolving DOD worldwide protected network allowing Warfighters to "plug in" and "push or pull" information in a seamless, interoperable and global battlespace.

DISN is a dynamic network, with the capability to accommodate emerging new or improved technologies that better serve the unique communication needs of the Warfighter. DISN provides seamless and interoperable information transport across strategic and tactical networks supporting Joint Task Forces and Combined Task Forces, as well as the telecommunications networks of non-defense agencies.

DISN will provide the transmission and switching of voice, data, video, and point-to-point bandwidth services for wide area, local area, metropolitan area, and long-haul networks.

DISN will use available commercial products and services, while providing DOD with the degree of network control necessary to ensure rapid response to the Warfighters. DISN integrated voice/imagery and data information transport will be transparent to the Warfighters, facilitate the management of information resources and be responsive to national security and defense needs under all conditions in the most efficient manner.

In early 1995, the Joint Chiefs of Staff (JCS) validated a Mission Need Statement (MNS) which realigns priorities from simple business-case services to a more secure and government controlled network of commercial switching nodes and leased transmission services. This focuses C4I more directly for the Warfighter.

In early 1996, the JCS issued a Capstone Requirements Document which clearly segments DISN into three distinct blocks. These blocks are base level, long-haul, and deployed. All blocks are to be implemented as fully interoperable blocks, but by different organizations, with the technical oversight of DISA. The Services will implement DISN on their respective bases, DISA will implement the long-haul block, and different Services or Agencies will be designated to jointly implement the deployed block.

Since July 1995 when the strategy was announced, DISA has awarded all four initial DISN contracts. The first contract, DISN Support Services - Global (DSS-G) contract, was awarded to Boeing Information Services, Inc. The DSS-G serves as the network's technical management support vehicle. The second contract, DISN Switched/Bandwidth Manager Services (DS/BMS-C), was awarded to MCI Telecommunications Corp and covers the continental United States (CONUS). In addition to supporting the vast majority of CONUS, this contract covers overseas traffic that originates or terminates in the 48 contiguous states.

The third contract, DISN Transmission Services - CONUS (DTS-C), was awarded to AT&T Government Markets. This contract will provide backbone and access area transmission services at T-1 and above bandwidth rates. The fourth contract, DISN Video Services - Global (DVS-G), was also awarded to AT&T Government Markets. AT&T will provide multi-vendor interoperability and dedicated video services including secure and non-secure, point-to-point and multi-point bridging, a reservation/scheduling system, video services management and monitoring, and provisioning and user-site network interface equipment.

DISA has also awarded the DISN Hawaii Information Transfer System (HITS) contract to AT&T Government Markets. This provides wide-area and local networking services to DOD facilities within the State of Hawaii.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of March 1997)

Defense Message System (DMS)

Summary

The Defense Message System (DMS) consists of all hardware, software, procedures, standards, facilities and personnel used to exchange electronic messages between organizations and individuals in the Department of Defense (DOD), whether at home base, while traveling or when deployed. The DMS baseline consists of the existing Automated Digital Network (AUTODIN) and electronic mail (e-mail) on the DOD Internet. It will provide a common messaging environment that is flexible and interoperable between the Services, Agencies, Joint Staff, Federal Agencies, our Allies, and the public.

Facts/Discussion

DMS was established to develop an integrated, common user, organizational and individual messaging and directory services system which satisfies validated requirements as identified in Multicommand Required Operational Capability (MROC) and Required Operational Messaging Characteristics (ROMC). In January 1993, the Defense Information Systems Agency (DISA) was tasked to assume lead agency role and program management of the DMS.

DMS's primary objective is to reduce cost and staffing by eliminating the resource-intensive and archaic AUTODIN, while the second objective is to improve support to the warfighters by implementing advanced messaging and directory service, building on mainline commercial products and incorporating international standards. To achieve these objectives, the following have been defined, validated and documented:

--A baseline from which proposed DMS costs and benefits could be measured,
--A target architecture which satisfies all validated DMS requirements, and
--An implementation strategy for the target architecture to evolve from the baseline.

The DMS Program is employing an innovative acquisition strategy designed to influence development of commercial mainline products while maintaining maximum competition and acquisition flexibility. Through this acquisition, vendors are encouraged to provide commercial product solutions to meet DOD's messaging, directory service, security and service management requirements.

Defense Information Systems Agency 701 S. Courthouse Road Arlington, VA 22204-2199

DMS will provide full range of messaging and directory services to globally dispersed users and will ensure essential characteristics including connectivity, interoperability, accountability, reliability and security.

DMS must be able to provide writer-to-reader messaging service access to and from worldwide DOD locations, including tactical deployed users and other designated members of the Federal Government.

Using the global Defense Information System Network (DISN) transmission system and supporting mission facilities utilized in the tactical environment, DMS will provide seamless messaging (X.400), directory (X.500), service management and security (Message Security Protocol) services for DOD organizations and individuals.

An Indefinite Delivery, Indefinite Quantity acquisition contract for DMS-compliant products and services was awarded to Loral Federal Systems (now Lockheed Martin Federal Systems) in May 1995, and the system is currently in its operational testing and evaluation phase. DISA adopted and the Military Communications Electronic Board has approved an event-driven fielding strategy with target dates.

Major capabilities are being defined in terms of criteria matched to tests that provide quantifiable metrics. This criteria-based approach applies Global Command and Control (GCCS) lessons learned. With approval of the Major Automated Information System Review Council, DMS has been installed at nine initial operational capability (IOC) sites.

The system is successfully exchanging signed and encrypted DMS messages using LOTUS, Microsoft, and ESL user agents and ESL infrastructure components. IOC for Sensitive but Unclassified messaging is projected for March 1997. More than 100,000 user agents have been ordered to date, and 215,000 users are projected to be in live operation by the end of CY 1997.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of January 1997)

Information Security (INFOSEC)

Summary

INFOSEC is the measures and controls that safeguard and protect an information system from unauthorized disclosure, modification or destruction from such threats as hackers, terrorists and foreign governments. The Defense Information Systems Agency, (DISA) as central manager of the Defense Information Infrastructure (DII) and in joint cooperation with the National Security Agency (NSA), defines INFOSEC requirements and implementation into the DII. The Defense Intelligence Agency (DIA) supports these activities with threat assessments.

Facts/Discussion

The DII is a seamless web of communications networks, computers, software databases, applications, facilities and other capabilities that meet the Department of Defense's (DOD) information processing and communications needs. Information systems cannot be protected with a single mechanism. DISA must ensure that the DII contains the adequate protection against attack by using a layered defense.

Under the Multilevel Information Systems Security Initiative (MISSI), NSA is developing a complete suite of security products which include the FORTEZZA family of crypto cards, firewalls and multilevel security guards/gateways which DISA is implementing to protect the DII. DISA is working to ensure that information security is integrated into all of its programs from the beginning.

The Global Operations and Security Center (GOSC) consolidates the functions of the Global Control Center and the Automated Systems Security Incident Support Teams (ASSIST) into one organization. This consolidates all aspects of security into the day-to-day management and operation of the networks supporting the Department of Defense. The center monitors, detects, and reacts to disruptions in the infrastructure. The center also includes daily operation of the Vulnerability Analysis and Assessment program (VAAP). This program provides an evaluation of the overall security posture of the DII by way of intrusion penetration testing. The Defense Intrusion Analysis and Monitoring Desk (DIAMOND) is located in the center and provides advanced analysis of intrusion data and network sensors looking for unauthorized activity. The GOSC also provides DOD-wide support for the detection, analysis and removal of malicious code (more commonly known as viruses, logic bombs, etc.).

The INFOSEC Program Management Office (IPMO) consolidates the acquisition, implementation, integration and dissemination of INFOSEC products and services

into the DISA pillar programs (e.g., DISN, DMS, GCCS, and GCSS) and other DOD systems and activities. The IPMO coordinates with the CINCs, Services and Federal Agencies to determine requirements and develop standardized INFOSEC tools, methods, and training and awareness products, which help to ensure the confidentiality, integrity and availability of warfighter information systems. The IPMO provides INFOSEC technical support functions to include INFOSEC certification, connection approval and compliance validation of connections to the DII. The IPMO also manages development and fielding of standard multilevel security capabilities supporting CINC, Service and Agency C4I requirements.

DISA supports Information Warfare - Defense activities of intelligence organizations, the CINCs Services, other Federal Agencies, and the private sector.

As of February 1997

Personnel and Manpower Directorate (D1)

Summary

D1's top priority is to ensure DISA/NCS has a highly skilled, well-trained team of professional men and women to meet the communications and computer systems needs of our Nation's warfighters. This is accomplished through an integrated system of recruitment, education, training, and administrative support. Postured with a team of approximately 10,300 military members and civilian employees stationed worldwide, the Agency exceeds customer expectations.

D1 assists the Director, DISA by developing, executing, and evaluating plans and programs guidance, including the Director's Human Resources Strategic Plan, a roadmap to one of the Agency's key successes.

Other D1 high priorities are to manage the extensive civilian intern employee recruitment of recent college graduates, targeted to fill key positions throughout the Agency primarily in technical disciplines; lead a DISA/NCS-wide education and training program using state-of-the-art technologies such as satellite broadcasts and video teleconferencing to keep employees in step with technology growth; and lead the development and implementation of the Career Management Systems in nine major career disciplines.

D1 is divided into these organizational elements:

--**Civilian Personnel Division,** provides guidance, assistance, and operational support to DISA/NCS employees worldwide on all aspects of the civilian workforce.

--**Military Personnel Division,** provides guidance, assistance, and support for Army, Navy, Air Force, and Marine Corp personnel assigned to DISA/NCS worldwide.

--**Personnel Systems Management Division,** provides Payroll support to all DISA/NCS civilian employees in the National Capital Region. Manages DISA/NCS civilian personnel data worldwide.

--**Organization and Manpower Division,** exercises centralized authority and accountability of DISA/NCS's organizational structure and related manpower authorizations. Facilitates management of organizational change, the Joint Manpower Program, and manpower budget.

--**Executive Services Division,** provides support operations for DISA/NCS's mail distribution, travel services, visual information, graphics, printing, and reproduction. Administers safety and occupational health programs.

--**Security Division,** provides security policy (except information systems security), guidance, and oversight for DISA/NCS activities worldwide; and supports security certification of systems and networks for DISA/NCS, DOD, and NATO.

--**Human Resources Development Branch,** provides comprehensive, DISA/NCS-wide plans, programs, and services for employee performance improvement and skill development aligned to the DISA/NCS mission. Major customer-focused areas include: Training and Development (Information Systems and Mission Support Careers), Career Development, Organization Development, and Business Operations.

For additional information

Contact DISA Public Affairs Office at (703) 607-6900.

(As of January 1997)

Command, Control, Communications, Computers and Intelligence (C4&I) Programs Directorate (D2)

Summary

D2 provides for the project management, technical development, and planning for life-cycle management of the DISA Pillar Programs: the Global Command and Control System (GCCS), the Defense Message System (DMS), the Defense Information System Network (DISN), the Global Combat Support System (GCSS), and Information Security (INFOSEC). D2 also ensures the cross-program integration of these programs into a seamless Defense Information Infrastructure (DII) for the warfighter.

D2 has responsibility, authority, and accountability for systems development, configuration management, integration, resource budgeting and execution, and product delivery; coordinates the talents and energies of engineering, testing, logistics, contracting, operations, and security functions to produce C4I for the Warrior capabilities as part of the integrated DII; and manages and trains Agency acquisition personnel.

Facts/Discussion

D2's objective is to be the provider of choice for development and acquisition management of information systems by ensuring technology projects and procurements are effectively and efficiently managed, by ensuring products are delivered on time and within budget, and by ensuring the customer is satisfied.

The Directorate strives to streamline, modernize and integrate C4&I information infrastructure and products to meet DOD requirements. Integration of C4&I programs into the DII is ensured by identifying and providing a horizontal, comprehensive perspective of high-level programmatic system and technical issues which cut across C4&I systems.

The following are the D2 organizational elements:

--**Defense Information System Network (DISN) Project Management Office,** provides definition, central integration and management of DISN, the end-to-end, seamless transport piece of the DII. Exercises the central planning, integration and coordinated execution of DISN component projects in response to Joint Staff validated requirements as quick reaction solutions.

--**Global Combat Support System (GCSS) Project Management Office,** works with the Joint Staff, Services and Agencies to provide a common integrated combat support environment with the objective to enable Joint Warfighter access to needed combat support information at anytime from any place from a single computer.

--**Global Command and Control System (GCCS) Project Management Office,** provides centralized management and control of development, integration, configuration management, quality assurance, testing and fielding of components that support validated command and control requirements. Coordinates the integration of selected Joint hardware, software, and communications equipment into an integrated command and control system for the warfighter.

--**Defense Message System (DMS) Project Management Office,** manages the transition and implementation of the DMS architecture throughout DOD. Provides program management of requirements, research, development, acquisition, product integration and fielding related to DMS.

--**Information Security (INFOSEC) Project Management Office (IPMO),** acquires, implements, and disseminates INFOSEC products and services for integration into the DII. Manages development and fielding of standard multilevel security capabilities supporting DOD C4I requirements. Determines, in coordination with CINCs, Services and Federal Agencies, requirements to ensure confidentiality, integrity and availability of DOD information systems. Provides standardized INFOSEC tools, methods, training and technical support functions to the DOD.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of February 1997)

Operations Directorate (D3)

Summary

D3 provides staff support to the DISA Director in centrally managing the entire Defense Information Infrastructure (DII), providing operational oversight, guidance, and support worldwide. It directs operation of the DISA portion of the DII, to include assigned portions of the command and control information systems operation, and monitors the efficiency and effectiveness of the warfighters' strategic C4I (Command, Control, Communications, Computers, and Intelligence) systems. The directorate coordinates the operational requirements of CINCs, Services, and other customers. Information technology services include communications, computers, and network systems management.

Facts/Discussions

The following are major functions performed by D3:

--**Customer Support and Operational Requirements,** focal point for corporate-level policy and coordination for support to warfighters and combat support organizations. Manages the Agency-wide operational requirements process. Identifies, communicates, and resolves CINC, Service, and Defense Agency operational requirements and issues.

--**Global Operations and Security**, center for 24-hour/day oversight, operations, and security of the DII. Executes management control and technical direction of the DII through system and network management for seamless, end-to-end integrity and responsive global C4I to the war fighter. Executes programs and initiatives to protect the DII against attacks.

--**DII Services,** provider of responsive, reliable, and cost-effective transmission and communication services. Manages bandwidth services, space and terrestrial transmission systems, router networks, and switched data networks. Installs, operates, maintains, and evaluates existing voice, video, messaging, and imagery information networks and systems making up the DISA-operated portion of the DII. Implements needed consolidations and upgrades.

--**Operational Plans and Policy**, principal staff office for all matters concerning operational plans, concepts, policies, and procedures for the DII. Exercises staff oversight to ensure global DII operational plans, policies, procedures, and training

are developed, reviewed, implemented, and maintained to support the operations and management of the DII. Develops and implements procedures for assessing the health of the DII to ensure maximum efficiency and effectiveness in meeting DII user needs. Institutes and coordinates the scheduled inspections for specific elements of the DII.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of March 1997)

Procurement and Logistics Directorate (D4)

Summary

D4 provides guidance on those issues that have logistic, procurement, real estate, and facilities implications. It develops and manages the DISA procurement system, evaluates procurement system performance, and develops the procurement and contracting work force. D4 provides logistic planning advice to the managers of DISA's major systems. It also provides facilities support for more than 120 locations on three continents.

Facts/Discussion

D4 provides policy guidance and oversight of DISA's procurement agent, the Defense Information Technology Contracting Organization (DITCO). DITCO is responsible for purchasing information technology, telecommunications, and related technical services for the President, the Military Departments and more than 65 other government agencies, as well as DISA customers.

D4 influences the life-cycle management of DISA's major systems by analyzing and determining appropriate maintenance strategies, manpower, and personnel as they relate to: logistics, supply, and support equipment needs; the depth and breadth of technical data, training and training support requirements; and the computer resources support infrastructure, facilities requirements; and design interfaces.

D4 also provides detailed planning and program execution for an initiative to further consolidate many DISA facilities in the National Capital Region. This consolidation will result in improved organizational effectiveness and cost savings.

D4 is divided into four divisions:

--**Procurement Management Division**, provides support to customers in defining acquisition strategies. Develops, manages and oversees the DISA procurement system. Provides contracting policy for purchases of supplies and services to meet warfighter needs. Evaluates procurement system performance and enhances career management of the acquisition work force.

--**Logistics Division**, provides logistics policy, contingency plans, logistical systems readiness support, and Integrated Logistics Support (ILS) to DISA activities. Provides logistics support to systems that are owned, operated and/or managed by

DISA. Also operates warehousing and internal supply activities in the National Capital Region (NCR).

--**Real Estate and Facilities Services Division,** provides a high quality work environment for DISA. Formulates and executes real estate and facilities plans and policies for the operation of DISA worldwide. Procures and allocates work space in the National Capital Region. Resolves environmental problems in and around DISA facilities.

--**Contract Technical Services Division,** coordinates and oversees the use of DISA's major technical service contracts and provides value-added link between customers, the contracting process, and contractors. Ensures task and delivery orders directed toward technical services contracts are evaluated to verify that technical standards and architectures are preserved.

For additional information

Contact DISA Public Affairs Office at (703) 607-6900.

(As of January 1997)

Strategic Plans and Policy Directorate (D5)

Summary

D5 was created to provide policy development, strategic planning, integrated program development and capstone architectures for the Director of the Defense Information Systems Agency (DISA). D5 ensures these efforts meet the C4I Warfighting and mission support needs of the Joint Staff, CINCs, Services and other DOD and Federal Agencies. D5 also acts as DISA's focal point for international Command, Control and Communications (C3) and for support to the intelligence community.

Facts/Discussion

D5's mission is to focus the Agency's efforts on activities and products that directly support the warfighter. The policy framework and architectural, planning and programming processes must connect logically to the corresponding activities on the Joint Staff, the Office of the Secretary of Defense, the Services, and the Agencies. The products of these processes must ensure accountability, include "buy in" by participants and have clear leadership mandates. D5 also ensures that intelligence community requirements are properly processed in DISA and promote the integration of intelligence and C2 capabilities.

D5 is divided into five divisions:

--**Policy Division**, coordinates policy development and international C3 issues within DISA. Responsible for DISA's charter and actions related to roles and missions of the Agency.

--**Architecture Division**, serves as the program manager for all DISA architecture activities, providing oversight and staff direction for the integrated Defense Information Infrastructure (DII) technical architecture and roadmap. Serves as the DISA focal point to the intelligence community.

--**Plans Division**, leads DISA strategic planning activities to provide the Agency's vision, direction, strategies and objectives. Responsible for the DII Master Plan production and coordination of Service/Agency plans.

--**Programs Division**, manages and facilitates the development of DISA/NCS Corporate Plan materials by the component organizations of DISA.

--**Strategic Business Analysis Division**, ensures that Agency goals and strategies are defined for Defense Business Operating Fund (DBOF) initiatives and are supported by underlying plans, rates, and program defense material. Serves as the Agency focal point for strategic DBOF planning for communications and the Defense Megacenters (DMCs). Orchestrates DBOF program defense with higher authorities. Oversees the mission-based panels, providing direction, and analytical and administrative support.

For additional information

Contact DISA Public Affairs Office at (703) 607-6900.

(As of January 1997)

Engineering and Interoperability Directorate (D6)

Summary

D6 is responsible for information systems engineering and interoperability support to all DISA programs, Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD[C3I]) directed initiatives, and other Director, DISA-coordinated efforts. D6 also has program, policy and resource authority over the Joint Interoperability and Engineering Organization (JIEO). Through JIEO, D6 provides information technology support over the full range of warfighter-to-mission support systems and components of the DISA-managed Defense Information Infrastructure (DII).

D6 is responsible for providing Department of Defense (DOD) information systems architectures and standards and hardware and software engineering to support the acquisition, implementation and integration of secure information systems that meet the needs of DOD users in peace and war.

Facts/Discussion

D6 serves as the principal staff officer on all matters concerning the engineering and interoperability of the DII and DISN. D6 is responsible for ensuring the provision of Information Systems (IS) engineering and interoperability support to all DISA programs, directed under the ASD (C3I) Information Management initiatives, and for such other programs or efforts directed by the Director, DISA.

D6 is also "dual hatted" as the Commander of the Joint Interoperability and Engineering Organization (JIEO) with full program, policy, and resource control. D6 exercises direct tasking authority over the JIEO Centers. Through JIEO, D6 supports the development, acquisition, implementation and integration of secure information systems that meet the needs of DOD users in peace and war.

D6 evaluates, engineers, and ensures delivery of an integrated Global Combat Support System (GCSS), combining infrastructure capability with combat support applications of the Services, Agencies, Combatant Commands, Joint Staff, and Principal Staff Assistants in the Office of the Secretary of Defense (OSD). D6 integrates counterdrug specific applications into the DII, executes an architectural development program leading to interoperability across law enforcement agencies, and provides life cycle support for ongoing DISA counterdrug programs.

D6 has seven divisions:

--**Resource Management Division,** is the principal advisor to D6 on all financial management, fiscal year corporate plans, budget planning and execution, and resource issues. It provides oversight and direction on contract administration, financial planning, and execution matters. It coordinates all financial resource issues with the DISA Comptroller and other staff activities as required.

--**C4I Engineering Management Division,** provides engineering management oversight for designated C4I programs and projects by coordinating engineering requests, proposals, and tasks across the DISA staff when the use of engineering services are required/involved. It provides engineering recommendations and technical integration to the D6 for C4I engineering task priorities.

--**Combat Support Systems Division,** provides engineering management, product delivery, and fielding of GCSS. This includes combat and service support applications, Electronic Commerce/Electronic Data Interchange (EC/EDI), and communications and computer infrastructures.

--**Counterdrug Integration Division,** serves as the sole focal point and office of record for all tasking actions assigned to DISA and the National Communications System (NCS) supporting the National Drug Control Program.

--**Special C4I Projects Division,** is responsible to D6 for providing engineering support for special projects such as the National Military Command Center, Airborne Systems, Joint Command and Control Technical Support, Joint Warrior Interoperability Demonstration (JWID) Project Office, and Contingency Operations.

--**Requirements Assessment and Issue Resolution Division,** assesses all C4I requirements documents (per DOD 4630) to ensure IS compatibility, interoperability, and technical integration. It acts as a catalyst for the timely resolution of C4I and Automated Information Systems (AIS) interoperability issues. It manages or provides support to forums identifying, tracing, and developing approaches to resolve critical interoperability integration issues. It coordinates NATO guidance packages and supports the Joint Staff's development of joint doctrine and joint publications for the employment of C4 systems.

--**Information Management Division,** executes the DISA information program across D6/JIEO, ensuring that Information System Security (ISS), Information Management (IM), and Information Resource Management (IRM) functions are carried out effectively and efficiently and in accordance with applicable laws and regulations. Special emphasis is given to ensuring the appropriate, timely and cost-effective safeguarding of all D6/JIEO information assets and effective financial and property management accountability for IT equipment and service acquisitions.

For additional information

Contact DISA Public Affairs at (703) 607-6900.

(As of February 1997)

ANNUAL DII CONFERENCE
Sheraton Premiere
Tysons Corner, Virginia

AGENDA FOR DAY 1
Monday, 7 April 1997

Time	Event	Speaker/Location
0630 - 0755	Check-in and Demo/Display Open	Junior Ballroom C, D & E
0755 - 0800	Administrative Remarks	Col Jakowatz DISA, D3 Grand Ballroon
0800 - 0805	Welcome	BG Meincke DISA, D3 Grand Ballroom
0805 - 0825	Opening Remarks	MG Kelley Vice Director, DISA Grand Ballroom
0825 - 0845	DII Overview	RADM Gauss DISA, D6 Grand Ballroom
0845 - 0930	GCCS Overview	RADM Gauss DISA, D6 Grand Ballroom
0930 - 0945	Break	
0945 - 1030	GCSS Overview	RADM Gauss DISA, D6 Grand Ballroom
1030 - 1145	DISN Programs	COL O'Meally DISA, D21 Grand Ballroom
1145 - 1315	Lunch	
1130 - 1730	Demo/Display Open	Junior Ballroom C, D & E

Sheraton Premiere
Tysons Corner, Virginia

AGENDA FOR DAY 1
(Continued)
Monday, 7 April 1997

1315 - 1700	Subconferences	Leader / Location
	-GCCS	Col Ottinger JSSC/Grand Ballroom A
	-DISN Transition	CAPT Lillard D36/Grand Ballroom B
	-IDNX Mgt Work Shop	Mr Weeks D344/Conference Room 9 (**Govt Only**)
	-COE Subconference 1	Mr Houston D6/Pavilion 22
	-COE Subconference 2	Mr Houston D6/Pavilion 21
	-GCSS- EC/EDI	Ms. DePalma, D22, D6, D3 /Pavilion 23 (**Segments of this session will be Govt Only sessions**)
	-DSN Issues	LTC Lynch D36/Mezzanine 2 **(Segments of this session will be Govt Only sessions.)**
	-DRSN Issues	Mr McLaughlin D36/ Mezzanine 3, (Mezzanine 4 & 5 reserved for follow-on discussions)
	-DISN Space; Vision	Col Linares D3, D2/ Conference Theater
	-IW-D/INFOSEC Program	Maj Handy D33/Conference Room 6
1715 - 1930	No Host Social	Capital Club, on the Mezzannie Level

ANNUAL DII CONFERENCE
Sheraton Premiere
Tysons Corner, Virgina

AGENDA FOR DAY 2
Tuesday, 8 April 1997

Time	Event	Speaker/Location
0700 - 0730	Demo/Display Open	Junior Ballroom C, D & E
0730 - 0830	INFOSEC Overview	Col Sweeder/COL Thomas DISA, D33/D25 Grand Ballroom
0830 - 0930	DII Control Centers	Mr. Lou Morgan DISA, D33 Grand Ballroom
0930 - 1000	DII Master Plan Update	Mr. Len Tabacchi DISA, D5 Grand Ballroom
1000 - 1015	Break	
1015 - 1100	DMS Program Status	CAPT Day DISA, D24 Grand Ballroom
1100 - 1200	Defense Megacenters	CAPT Harms DISA, WESTHEM Grand Ballroom
1200 - 1330	Lunch	
1130 - 1730	Demo/Display Open	Junior Ballroom C, D & E

ANNUAL DII CONFERENCE
Sheraton Premiere
Tysons Corner, Virgina

AGENDA FOR DAY 2
(Continued)
Tuesday, 8 April 1997

1330 - 1700	Subconferences	Leader / Location
	-DISA CINC FLD CMDRs Meeting	MG Kelly /Daniel M. Ross Boardroom
	-DII Control Centers	Mr Morgan D33/Grand Ballroom A
	-DII Policy, Management, & Planning Initiatives	Mr Tabacchi D5/Grand Ballroom B
	-COE Subconference 1	Mr Houston D6/Pavilion 22
	-COE Subconference 2	Mr Houston D6/Pavilion 21
	-DMS	Ms Setz D2/Pavilion 23
	-DSN, DISN VTC & DISN OCONUS	LTC Lynch D36/Mezzanine 2
	-DRSN Issues	Mr McLaughlin D36/ Mezzanine 3, (Mezzanine 4 & 5 reserved for follow-on discussions)
	-IW-D/INFOSEC Program	Mr Horvath D25/Conference Room 6
	-DMCs	Mr A. Rivera WESTHEM/ Pavilion 25 (**Govt Only**)

ANNUAL DII CONFERENCE
Sheraton Premiere
Tysons Corner, Virgina

AGENDA FOR DAY 3
(Continued)
Wednesday, 9 April 1997

Time	Event	Speaker/Location
1000 - 1015	STRATCOM	Mr. Larry Ramsey J61, STRATCOM Grand Ballroom
1015 - 1030	USA	Mr John Saputo DISC-4, US Army Grand Ballroom
1030 - 1045	USN	CDR Crownover N62, US Navy Grand Ballroom
1045 - 1100	USMC	Col Bouldry HQMC, C4I Grand Ballroom
1100 - 1130	USAF	Mr James SCT, USAF Grand Ballroom
1130 - 1300	Lunch	
1130 - 1730	Demo/Display Open	Junior Ballroom C, D & E

ANNUAL DII CONFERENCE
Sheraton Premiere
Tysons Corner, Virginia

AGENDA FOR DAY 3
Wednesday, 9 April 1997

Time	Event	Speaker/Location
0700 - 0730	Demo/Display Open	Junior Ballroom C, D & E
0745 - 0800	CENTCOM	BG Harry D. Raduege, Jr J6, CENTCOM Grand Ballroom
0800 - 0815	EUCOM	LTC Thomas Jones ECJ6, EUCOM Grand Ballroom
0815 - 0830	SOCOM	Col Giampaolo J6P, SOCOM Grand Ballroom
0830 - 0845	PACOM	Col Thomas Hickerson J60, USCINCPAC Grand Ballroom
0845 - 0900	SOUTHCOM	BG Peter Cuviello Director, SCJ6 Grand Ballroom
0900 - 0915	ACOM	BG John P Cavanaugh J6, USCINCACOM Grand Ballroom
0915 - 0930	TRANSCOM	Col Thompson Deputy J6 Grand Ballroom
0930 - 0945	SPACECOM	Col John Maluda J6, SPACECOM Grand Ballroom
0945 - 1000	Break	

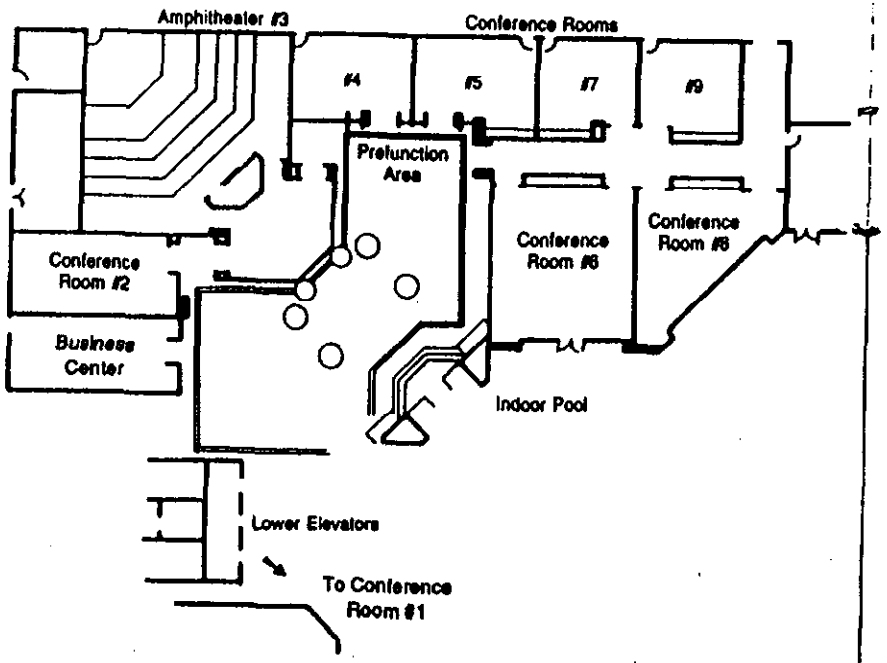
ANNUAL DII CONFERENCE
Sheraton Premiere
Tysons Corner, Virgina

AGENDA FOR DAY 3
(Continued)
Wednesday, 9 April 1997

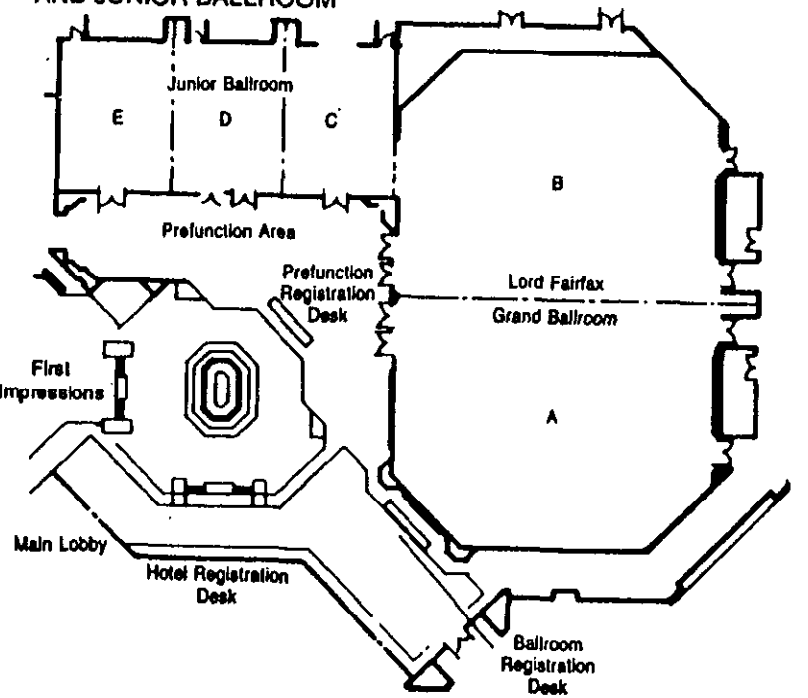
1300 - 1530	Subconferences	Leader / Location
	-DISN Space; Operations	LtCol Tomas D2/D3 Grand Ballroom A
	-DISN Data Networks	Mr Boyd D36/Grand Ballroom B (**Govt Only**)
	-COE Subconference 1	Mr Houston D6/Pavilion 22
	-COE Subconference 2	Mr Houston D6/Conference Theater
	-DMS	Ms Setz D2/Pavilion 23
	-DSN	LTC Lynch D36/Mezzanine 2
	-DRSN & DISN MONIES	Mr McLaughlin D36/ Mezzanine 3, (Mezzanine 4 & 5 reserved for follow-on discussions)
	-IW-D/INFOSEC Program	Mr Horvath D25/Conference Room 6
	-OS 390	Ms Englert WE31/ Conference Room 7

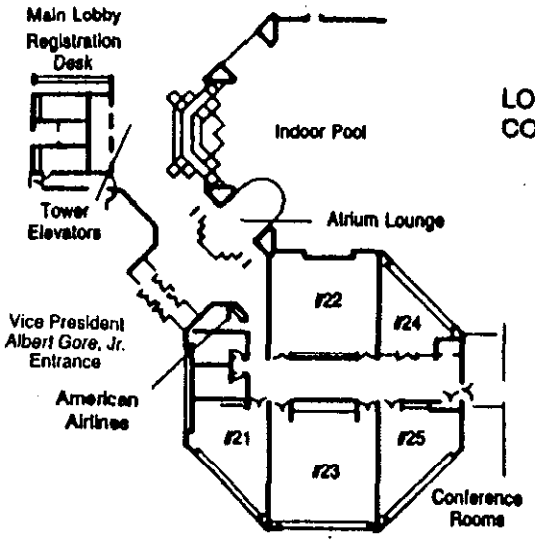
Time	**Event**	**Speaker/Location**
1530 - 1615	Subconference Report	Subconference Leaders Grand Ballroom
1615 - 1630	Closing Remarks	LtGen Edmonds Director, DISA Grand Ballroom

FIRST LEVEL

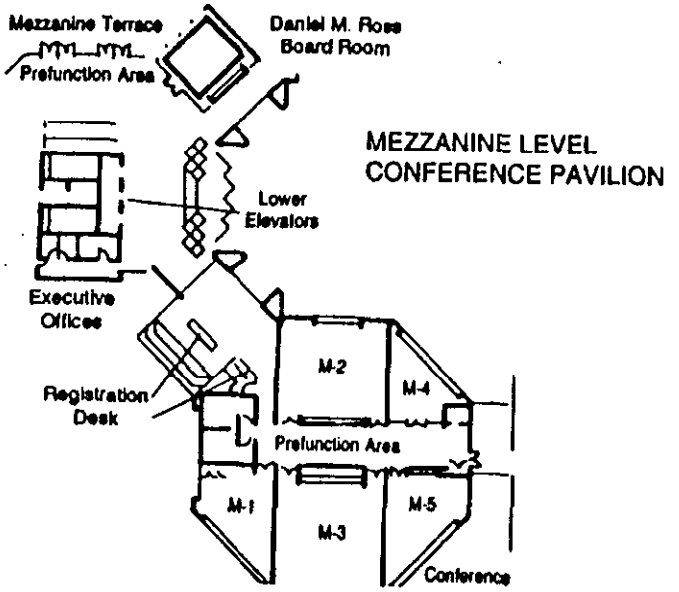


LOBBY LEVEL
GRAND BALLROOM COMPLEX
AND JUNIOR BALLROOM





LOBBY LEVEL
CONFERENCE PAVILION



MEZZANINE LEVEL
CONFERENCE PAVILION

The Defense Information Systems Agency

Presents

the

ANNUAL DEFENSE INFORMATION INFRASTRUCTURE (DII)

CONFERENCE

7 -9 APRIL 1997

We are looking forward to your participation in the Annual Defense Information Infrastructure (DII) Conference at the Tyson's Corner Sheraton Premiere, 8661 Leesburg Pike, Vienna, VA 22182. The objective of the Conference is to baseline the participants on DII development to date and to get customer inputs to ensure that the way ahead is on track to support Warfighter requirements. This once-a-year event will highlight GCCS, GCSS, DMS, INFOSEC, DISN/DII, DRSN, DSN and DISN-SATELLITE.

A large block of rooms has been reserved at the conference hotel. Please contact them for reservations at 703/448-1234 or fax 703/893-8193. Please complete the registration form shown below and press the SEND button to register. Additionally, we will require verification of your security clearance. Please fax a copy of a DISA Form 43 or equivalent local visit notification form to D3 Conference Coordinator, 703/607-4106, DSN 327-4106. Upon receipt of your registration form and your faxed security form, you will receive a letter of confirmation, which will include the emergency phone numbers, fax numbers and a Conference admission ticket. Thank You, and we look forward to seeing you at the Annual DII Conference.

Questions?

You can reach the D3 Conference Coordinator at: Conference Phone: 703/607-6514 - DSN 327-6514

Conference Fax: 703/607-4106 DSN 327-4106

Conference Email: confered@ncr.disa.mil ("DISA Conference" on the DISA LAN)

To Access the Automated DII Conference Registration form - click here

You will need to download the Visit Notification Form (DISA Form 43) and the Exemption Certificate (DISA Form 204)- click here

Please fill them out and FAX them to (703)607-4106 (DSN) 327-4106

Last Revision -13Feb 97 *west1c@ncr.disa.mil*

--
Donna Egner
WL/FIVS/SURVIAC Bldg. 45
2130 Eighth St. Ste 1
Wright Patterson AFB OH 45433-7542
Comm (937)255-4840
DSN 785-4840
Fax (937)255-9673
Email egner_donna@bah.com

Downloading & Downloading Instruction Page

For The DII Conference

Web browsers provide a *Load Files to Disk* option to download the selected files to disk instead of displaying them. While this option is in effect, all files selected will be downloaded to a default directory, designated within the browser itself, on the hard drive.

Most browsers also support another method, involving a **Shift-click** keyboard shortcut. This method will allow the user to designate a directory for the files to be downloaded to. First hold down the **Shift** key and then click on the file to be downloaded. A window should pop up that allows the user to select the disk and the directory to which the file will be downloaded.

This method is recommended for downloading all files from this Page

Some browsers also support a third method which can be used to download only the file that is currently being viewed by the browser at that given point in time. The user must select the *Save File* option located under the files menu bar item.

To Download DII Registration Form - WordPerfect 6.1 version - shift-click here

To Download DII Registration Form - MS Word 2.x version - shift-click here

To Download DII Registration Form - Text version - shift-click here

To View the DII Registration Form - shift-click here

To Download Visit Notification (DISA Form 43) in:

- WordPefect 6.1 format - shift-click here

- MSWord 2.x format - shift-click here

- GIF format - shift-click here

To Download Tax Exemption Certificate (DISA Form 204)in:

- WordPefect 6.1 format - shift-click here

- MSWord 2.x format - shift-click here

- GIF format - shift-click here

You will need to download the Visit Notification Form (DISA Form 43) and the Exemption Certificate (DISA Form 204) - *Please fill them out and FAX them to (703)607-4106 (DSN) 327-4106*

STOP

If You Used the *"Load to File"* option, Don't Forget to "Turn It Off"!!!!

Return to:
DII Conference Home Page
D31 Home Page
DISA Home Page

Last Revision -13 Feb 97 Chris West

Message for Benkert Jack

From: Chrisan Herrod

Date: Tue, Mar 18, 1997 1:29 PM

Subject: Red Team Briefing

To: benkert_jack@bah.com; surviac@bah.com; grubart@ncr.disa.mil

Jack, following up on our discussions with you last Friday, I would like to schedule a time to brief DISA and NSA folks on your Red Teaming activities, I also want to discuss your supporting a Red Team Workshop thru your IATAC contract.

My secretary is Tracy Grubar and she will arrange with key players calender. She can be reached at 681-7900. She will be on leave all next week so try and get to her this week to arrange.

I am also extending an invitation to you or someone you designate to attend the DII Subconference on INFOSEC/IWD. Please get with my POC John Horvath and arrange. He or Tracy can register you. ( )

Best time to try and get it together is April 4th or perhaps the 3rd at Skyline 4, 4th floor.

Tracy we will need to invite Col Thomas, JP, Eller, Bieber, actually all IPMO folks who are interested. And NSA Col. Marti Winters as well as Jim Sweeder and his folks, see what you can do. Brad Dement, need Time

thanx. chrisan

---------- RFC822 Header Follows ----------
Received: by smtpmac4.bah.com with ADMIN;18 Mar 1997 13:29:45 -0500
Received: from hail.ncr.disa.mil (hail.ncr.disa.mil [164.117.176.115]) by booz-mail.bah.com (8.8.5/8.7.3) with ESMTP id NAA27298; Tue, 18 Mar 1997 13:21:13 -0500 (EST)
Received: from ncr.disa.mil ([164.117.176.106]) by hail.ncr.disa.mil (8.7.3/DISA 8.7.3.01) with SMTP id NAA17571; Tue, 18 Mar 1997 13:19:39 -0500 (EST)
Received: from ccMail by ncr.disa.mil (SMTPLINK V2.11.01)
 id AA858720004; Tue, 18 Mar 97 13:17:00 EST
Date: Tue, 18 Mar 97 13:17:00 EST
From: "Chrisan Herrod" <herrodc@ncr.disa.mil>
Message-Id: <9702188587.AA858720004@ncr.disa.mil>
To: benkert_jack@bah.com, surviac@bah.com, grubart@ncr.disa.mil
Subject: Red Team Briefing

Defense Information System Network (DISN)

Overview

DISA's Defense Information System Network (DISN)—a $400 million initiative—provides an end-to-end information service to support critical national defense operations. Over 600 military installations nationwide will benefit into the next century from DISN's full range of information services. Awarded to MCI in August of 1996, the implementation of the DISN Switched/ Bandwidth Manager Services–CONUS (DS/BMS-C) program is being managed by the Government Markets Program Management Office (PMO).

MCI's DISN Partners

Due to DISN's stringent needs for network management, configuration management and control, and security assurance, MCI conducted an extensive search before selecting five industry leaders as its team members. NORTEL and Tellabs were selected to provide the DMS-100 switches and SONET bandwidth managers (BWM).
I-NET brings its experience in implementing integrated network management systems to the partnership, while Stonehouse is helping the team to meet the provisioning and reporting requirements of the DS/BMS-C program. Data Systems Analysts was selected because of its DISA security experience and ability to successfully navigate security accreditation.

Technical Solution

MCI's technical solution provides the Department of Defense with the required switched and bandwidth management services throughout CONUS. The SONET-based transmission backbone network is comprised of 35 SONET BWM sites using Tellabs' TITAN 5500s. Twelve of these sites also use the NORTEL DMS-100 switches to support circuit switching voice, data, and video services.

Implementation Challenges

DISN transition activities are being planned and managed by the PMO's implementation group. The group has two primary implementation responsibilities. The first is to provide the services of 12 switches and 35 bandwidth managers—ready to accept service connections—during May 1997. MCI must install and test this equipment, and have a redundant network management system in place by the required IOC date. The second implementation challenge is to achieve cutover of the existing DTC Network to the new DSS.

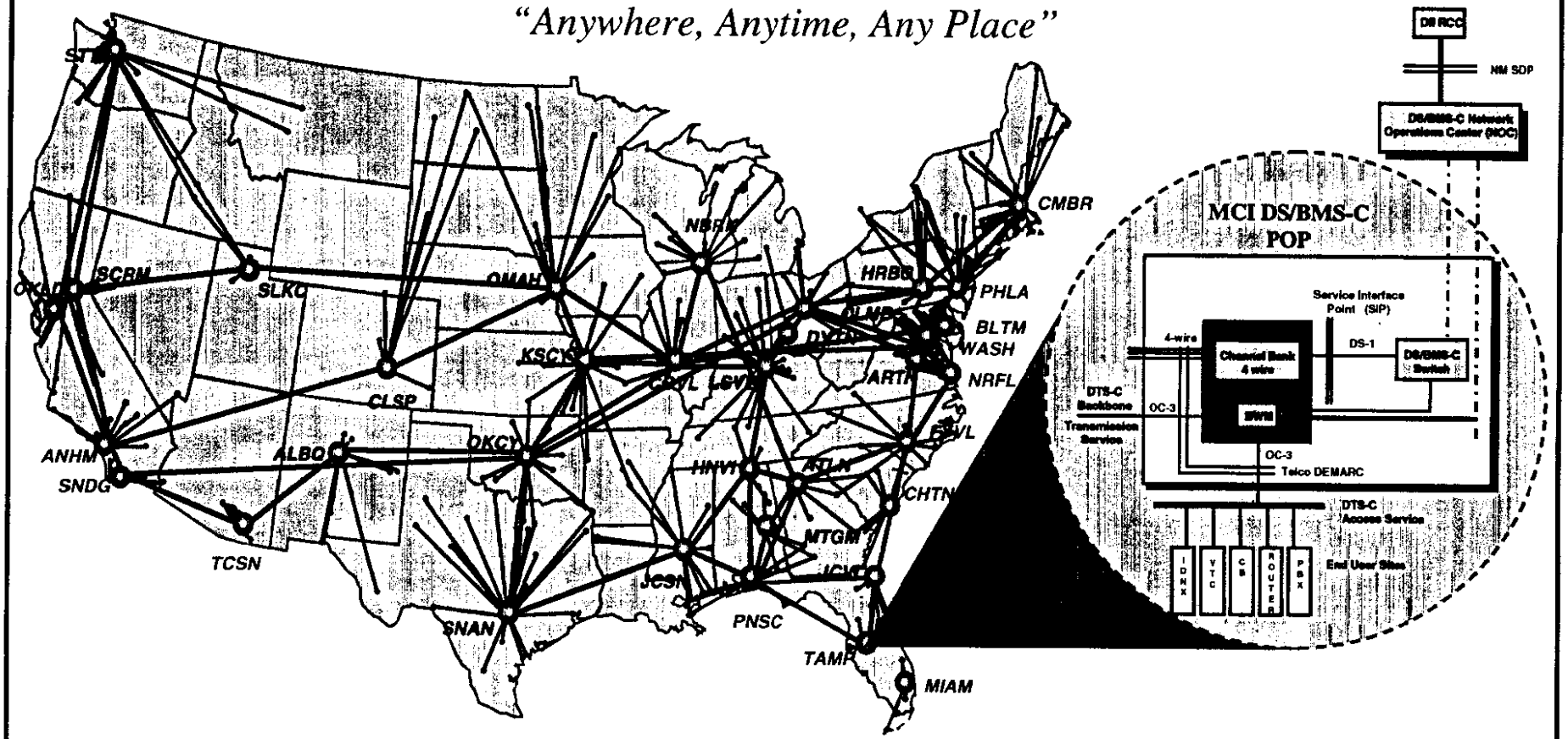
Summary

MCI's experience in transitioning customers from AT&T to MCI service will be key as the team works to meet the Government's aggressive timelines for DISN transition and avoid service interruptions. With the completion of DS/BMS-C, MCI will become a prime telecommunications provider for the DoD.

MCI DISN Switched/Bandwidth Manager Services

Global Communications Services for the Warfighter

"Anywhere, Anytime, Any Place"



35	BANDWIDTH MANAGER LOCATIONS
600	USER GEOLOCS
84	T3 ACCESS CIRCUITS
4,375	T1 ACCESS CIRCUITS
88	OC3 BACKBONE CIRCUITS

35 MCI Points of Presents & Network Operations Center providing:

- Bandwidth Management & Switching Services
- Security & Network Management
- Customer Services

Defense Information System Network (DISN)

Overview

DISA's Defense Information System Network (DISN)—a $400 million initiative—provides an end-to-end information service to support critical national defense operations. Over 600 military installations nationwide will benefit into the next century from DISN's full range of information services. Awarded to MCI in August of 1996, the implementation of the DISN Switched/ Bandwidth Manager Services–CONUS (DS/BMS-C) program is being managed by the Government Markets Program Management Office (PMO).

MCI's DISN Partners

Due to DISN's stringent needs for network management, configuration management and control, and security assurance, MCI conducted an extensive search before selecting five industry leaders as its team members. NORTEL and Tellabs were selected to provide the DMS-100 switches and SONET bandwidth managers (BWM).
I-NET brings its experience in implementing integrated network management systems to the partnership, while Stonehouse is helping the team to meet the provisioning and reporting requirements of the DS/BMS-C program. Data Systems Analysts was selected because of its DISA security experience and ability to successfully navigate security accreditation.

Technical Solution

MCI's technical solution provides the Department of Defense with the required switched and bandwidth management services throughout CONUS. The SONET-based transmission backbone network is comprised of 35 SONET BWM sites using Tellabs' TITAN 5500s. Twelve of these sites also use the NORTEL DMS-100 switches to support circuit switching voice, data, and video services.

Implementation Challenges

DISN transition activities are being planned and managed by the PMO's implementation group. The group has two primary implementation responsibilities. The first is to provide the services of 12 switches and 35 bandwidth managers—ready to accept service connections—during May 1997. MCI must install and test this equipment, and have a redundant network management system in place by the required IOC date. The second implementation challenge is to achieve cutover of the existing DTC Network to the new DSS.

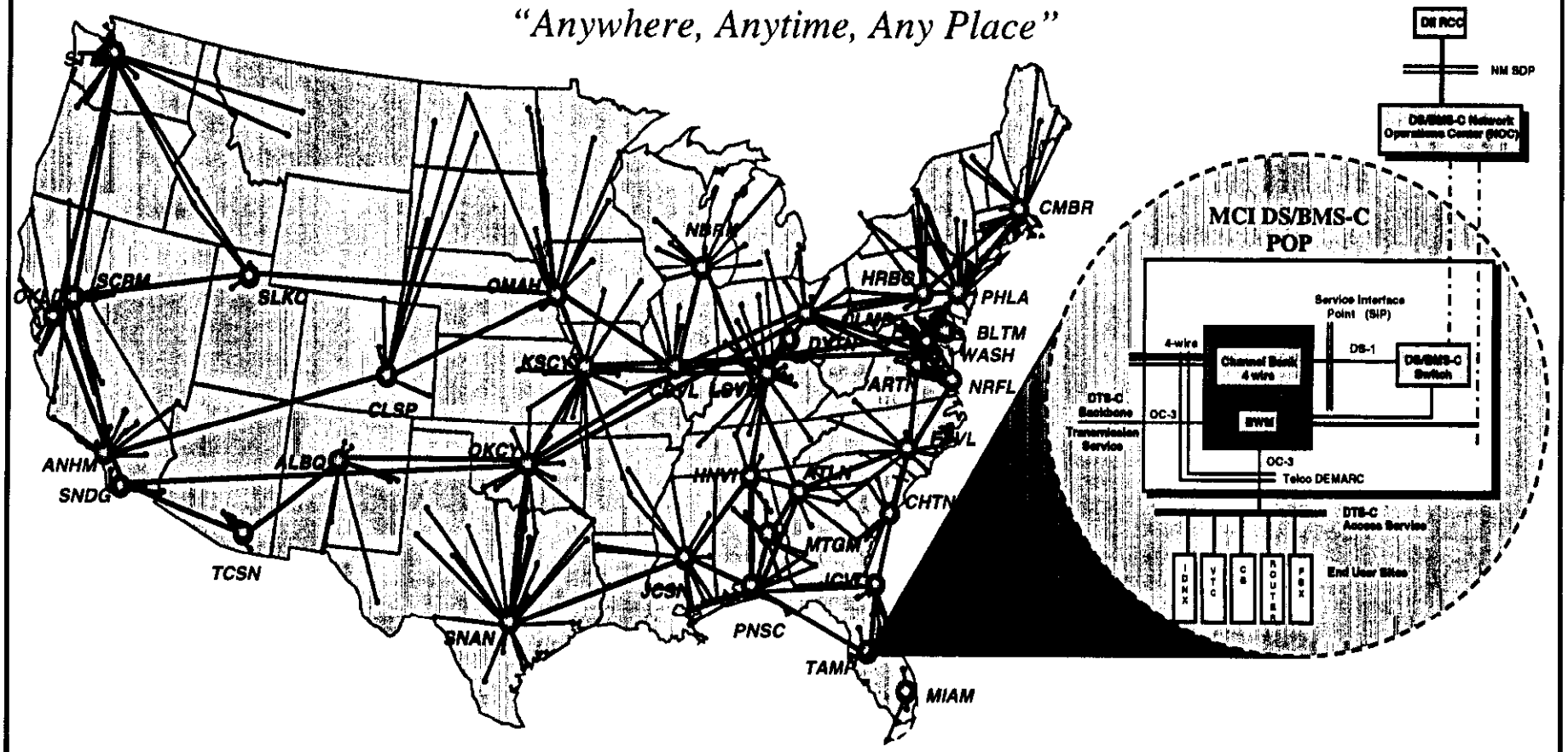
Summary

MCI's experience in transitioning customers from AT&T to MCI service will be key as the team works to meet the Government's aggressive timelines for DISN transition and avoid service interruptions. With the completion of DS/BMS-C, MCI will become a prime telecommunications provider for the DoD.

MCI DISN Switched/Bandwidth Manager Services

Global Communications Services for the Warfighter

"Anywhere, Anytime, Any Place"



35	BANDWIDTH MANAGER LOCATIONS
600	USER GEOLOCS
84	T3 ACCESS CIRCUITS
4,375	T1 ACCESS CIRCUITS
88	OC3 BACKBONE CIRCUITS

35 MCI Points of Presents & Network Operations Center providing:

- Bandwidth Management & Switching Services
- Security & Network Management
- Customer Services

A Tradition of Service

10400 Eaton Place, Suite 500
Fairfax, VA 22030
TEL 703/591-3704
FAX 703/591-8418

4300 Haddonfield Road
Pennsauken, NJ 08109
TEL 609/665-6800
FAX 609/665-6672
info@dsainc.com

2350 Lakeside Blvd., Suite 850
Richardson, TX 75082
TEL 214/238-8680
FAX 214/783-9755

Data Systems Analysts, a World-Leader for over 30 Years

DSA has been at the forefront of aeronautical messaging technology for over three decades:

Teamed with Philips of North America, DSA designed, implemented, and installed the North American Data Interchange Network (NADIN I). This network, the biggest of its kind, consists of two very large-scale AFTN centers and approximately 50 concentrators. It forms the backbone message switching network for the U.S. Federal Aviation Authority, delivering thousands of flight plans, notices to airmen (NOTAMS), and weather bulletins daily.

DSA has successfully developed and delivered over twenty aeronautical message switches throughout the world handling AFTN, IATA (ICM/B), meteorological, and X.400 messages - often with network interoperation.

Airline message switching for SITA, ARINC, and airlines include: multi-way gateways, backbone switches, and custom interfaces.

In conjunction with message handling, DSA has provided specialized data bases and interfaced with networks for MET, OPMET, Flight Plans, MOTNE, and ROBEC.

Hardware Specifications

Processor:	**1-32 Intel Pentium processor configurations**
Memory:	**32MB standard (expandable to 128MB) per processor**
Disk Store	**1 gigabyte standard (expandable to 12 gigabytes)**
Fault Tolerant:	**Load sharing and standby fault tolerance available in multi-processor configurations**
	- RAID levels 1 and 5 (optional) disk storage
	- Duplicated file server (optional)
Tape Storage:	**5 gigabyte DAT standard**
Circuits:	**8 asynchronous, 1 synchronous standard (expandable to 1024 asynchronous, 32 synchronous)**

Gateways/Access Units Available

Microsoft Mail

TCP/IP suite, including SMTP

cc:Mail

Telex

Lotus Notes

FAX (transmission and reception)

IBM PROFS

WordPerfect Office

Communications Protocol Support

AFTN (ICAO Annex 10)

IATA (ICM/B)

X.25 Synchronous (9.6k - 64k baud)

Asynchronous (50 - 19.2k baud)

X.400

Ethernet

Facilities and Features

A•MHS includes a rich set of facilities and features tailored to the needs of civil aviation. These include:

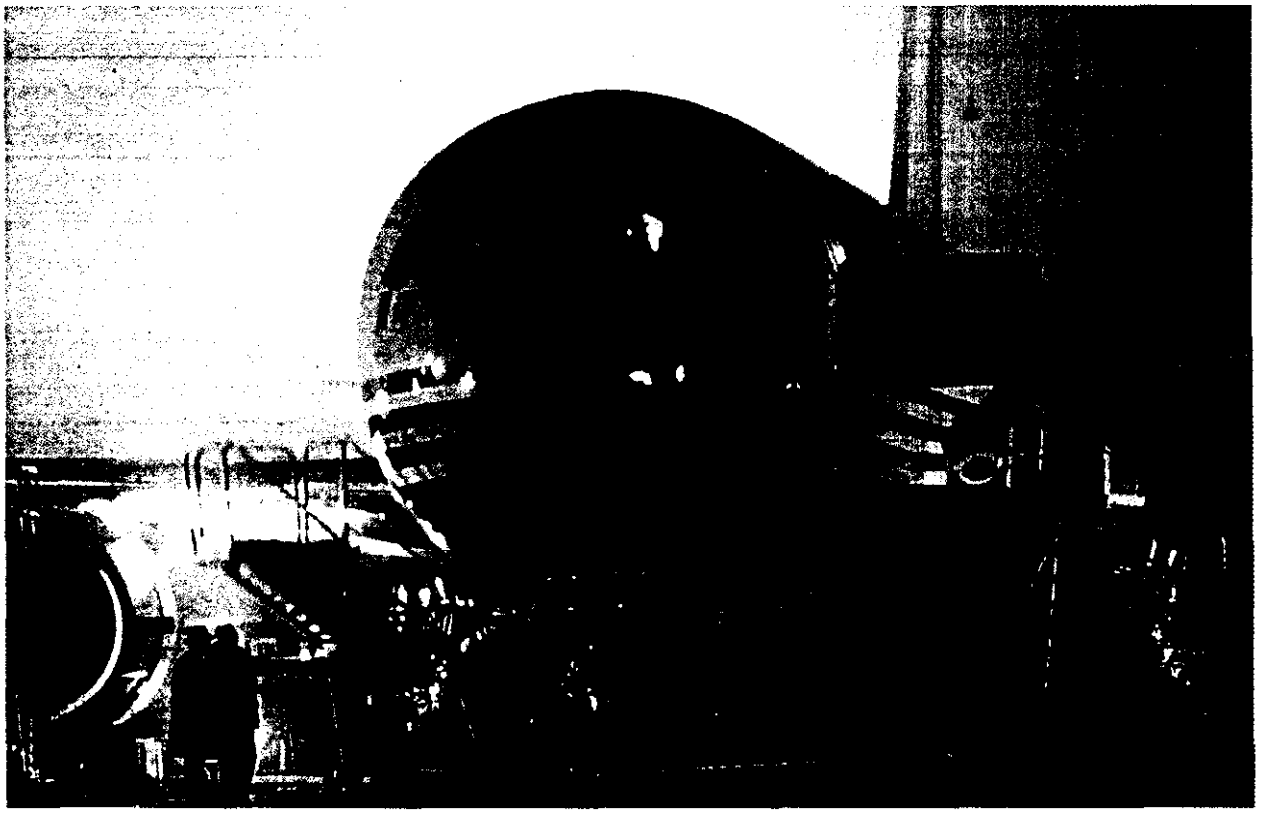
- Priority grade message handling
- Message archiving (short-term on disk and long-term on tape)
- Alternate routing
- Message tracing
- Message retrieval/re-send
- Directory-based routing
- Message correction/repair
- Channel sequence number error detection
- Automatic delivery retries
- Automatic service message generation
- Reports and alarms
- Collective (distribution) recipient lists
- Automatic system re-start/fail-over

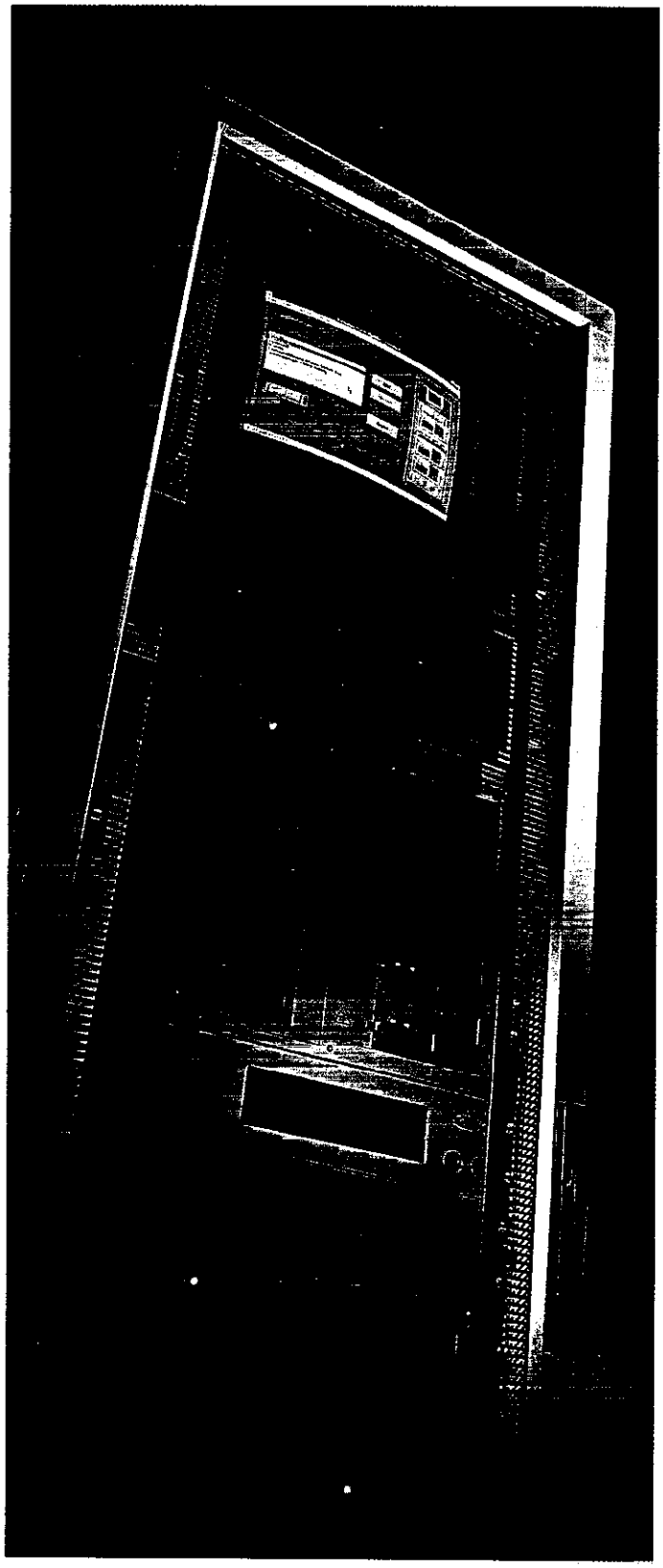
A Bridge To The Future

Modern standards, such as X.400, will, over the course of time, enable civil aviation authorities and others in the air transportation industry to offer new services far beyond simple message switching.

Of course, **A•MHS** is ready today with full support for X.400, as well as the increasingly popular LAN-based electronic messaging environments, such as Microsoft Mail, Lotus Notes, and Lotus cc:Mail.

The **A•MHS** "multi-way" gateway feature enables users to exchange messages with legacy systems, standards-based networks, and proprietary networks. In addition, this exchange could be accomplished using a single multi-addressed message. For example, a Lotus Notes user could address a single message to an AFTN destination, a user on a LAN using Da Vinci Mail at a distant office, an X.400 user in the ATN, and copy another user via FAX.





Message Accountability

In civil aviation, you need to know when a message was received, when and where it was delivered, and most importantly, be able to prove it.

***A•MHS** includes superior message archiving, logging, and trace facilities which set it apart from other systems.*

Reliability

When it comes to providing dependable products, used for around-the-clock messaging service - no one understands the issues better than ***DSA.***

A•MHS *offers extremely high reliability, availability, and message integrity. This is achieved using a redundant hardware architecture, a fault-tolerant software design, backed by years of corporate experience designing, implementing, and maintaining mission critical messaging systems and networks.*

A Highly Scaleable System

There is no such thing as outgrowing **A•MHS!** A system may be configured to run on a single processor with a small number of communications lines, and as traffic increases, additional processors and lines may be added to the configuration for minimal cost.

Commercially Available Hardware Components

Gone are the days of expensive, customized hardware for messaging that often locked organizations into a single vendor.

A•MHS is built entirely upon readily available, off-the-shelf components which offer huge price/performance advantages expected to last well into the next century. For example, a rack-mounted configuration using Compaq hardware is shown at right.

Ease of Operation

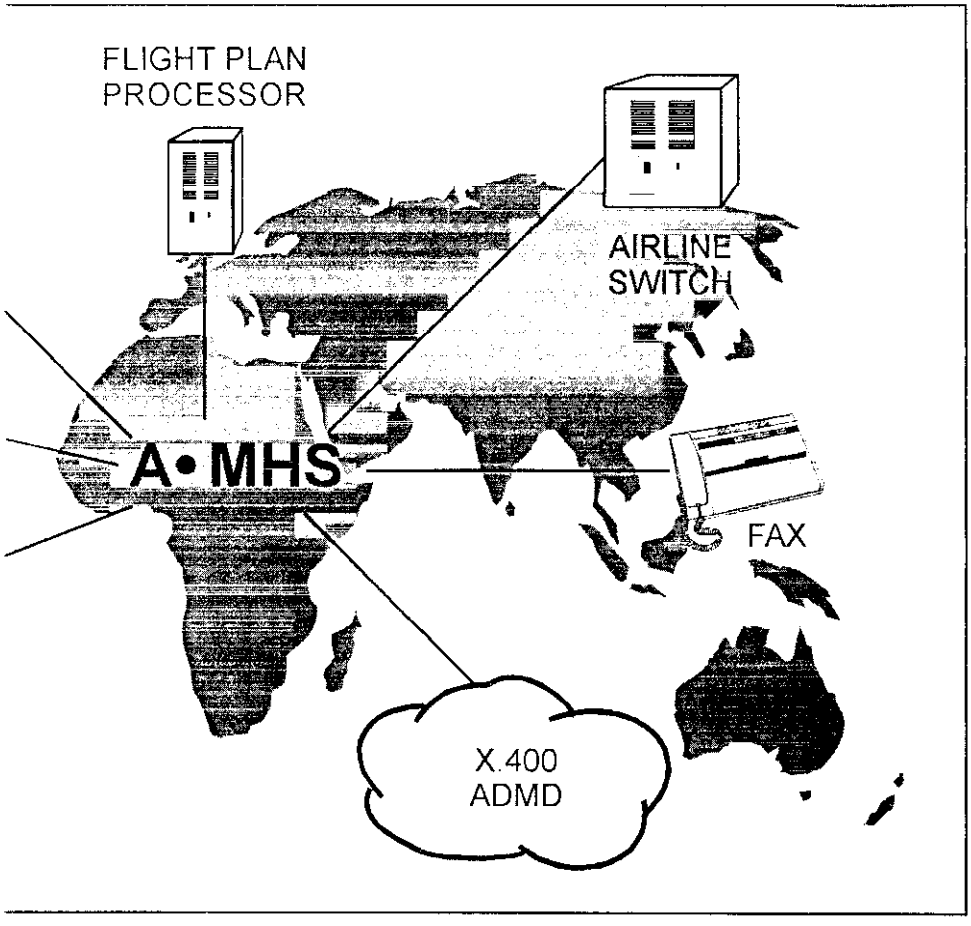
A•MHS is designed to run unattended for extended periods of time. However, when manual intervention is required, the system administrator can perform the tasks without extensive training or experience.

A•MHS provides graphical user interfaces, with mouse support, as well as a high degree of automation to help operators complete their job efficiently and easily.

Extraordinary Performance

A•MHS is the first aeronautical message switching product to truly take full advantage of these trends. Hardware and software components can be distributed across a series of processors, linked together via a high-speed backbone. This allows for an array of possible configurations and amazing flexibility during the lifetime of a system.

A•MHS multi-processor systems are implemented in a fully integrated, cabinet-style configuration that houses rack-mounted processors. Single processor systems (for example, gateways and concentrators) are implemented on tower-form servers.



A•MHS *leaves ordinary message handling systems far behind when it comes to performance. It was designed by a team of engineers who specialize in providing solutions used to move thousands of messages around the globe in seconds. Its scaleability allows unlimited upward growth to meet any throughput level required.*

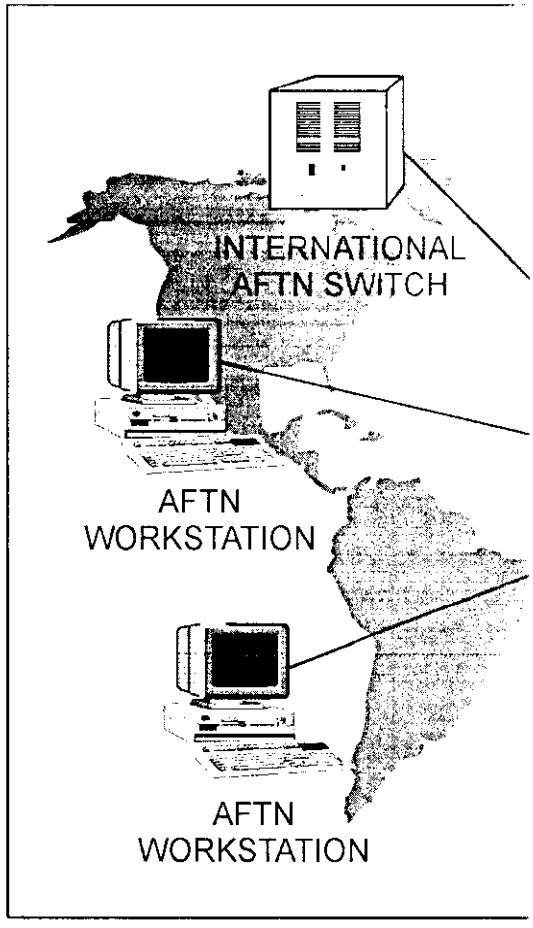
A•MHS

Aeronautical Message Handling and More

The air transport industry presents unique challenges which ordinary message handling products cannot meet. Reliability, performance, and a rich set of operational features are not just a requirement - they are essential to the safety of the many millions of passengers who fly each year.

For environments such as these, **DSA**, a world leader in secure messaging systems for more than three decades, offers the Aeronautical Message Handling System (**A•MHS**).

A•MHS is a fully functional AFTN and ATN-ready store-and-forward message switching system capable of interoperating with other types of networks. It offers the most cost effective solution available today! The system is designed to take advantage of the latest developments in client/server computer architecture and at the same time fulfills even the most demanding needs.



Flexible Client/Server Architecture

Many organizations are now downsizing from mainframe and mini-computer based systems to client/server architecture. The reasons are simple: price, flexibility, and ease of maintenance.

Standards

*The **A•MHS** conforms to the standards applicable to the connected message environment, including: ICAO, ATA/IATA, ITU (CCITT), Internet RFCs, and commercial product standards. Not only are the message handling procedures and protocols included, but also the major industry APIs (application program interfaces) such as VIM, MAPI, and CMC. This facilitates integration with networks, message switching systems, and software packages.*

A • MHS Backbone

Aeronautical Message Handling System

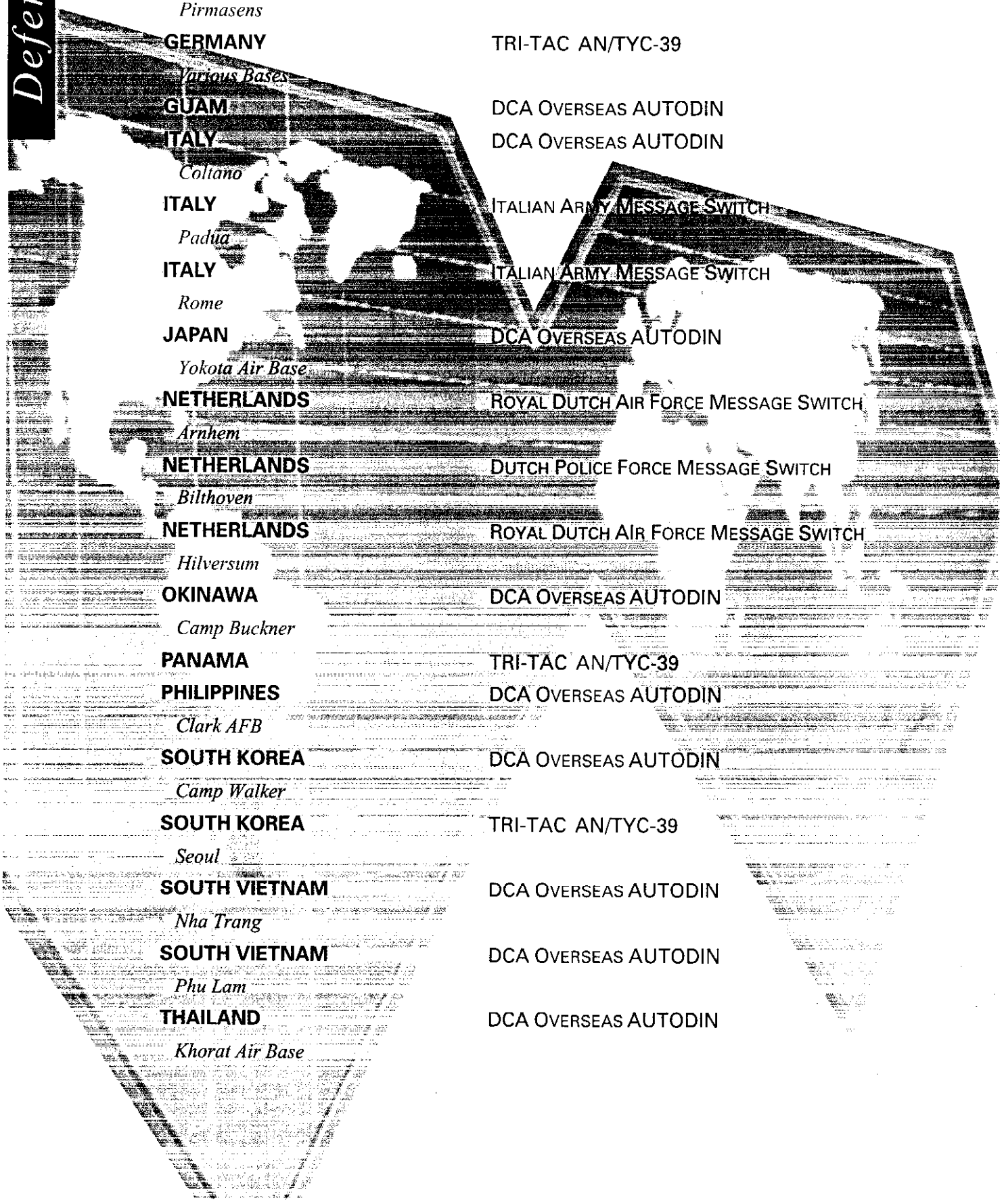
DATA SYSTEMS ANALYSTS, INC.

A Tradition of Service

AUSTRIA *Vienna*	INTERNATIONAL TELEGRAM FOR RADIO AUSTRIA
BRAZIL *Rio de Janeiro*	LEASED CHANNEL FOR EMBRATEL
BRAZIL *Rio de Janeiro*	INTERNATIONAL TELEGRAM FOR EMBRATEL
CANADA *Montreal*	PACKET SWITCH FOR CANADIAN NATIONAL/CANADIAN PACIFIC
COSTA RICA *San José*	ELECTRONIC MAIL FOR INTERNATIONAL CARRIER (RACSA)
ENGLAND *London*	INTERNATIONAL TELEGRAM FOR BRITISH POST OFFICE
FRANCE *Paris*	IATA MESSAGE FOR SITA
GERMANY *Manheim*	X.400 FOR INTERNATIONAL ELECTRONIC MAIL FOR DEUTSCHES BUNDEPOST
GERMANY *Munich*	SATELLITE EARTH STATION DEVELOPMENT FOR DEUTSCHE FERNMELDE SATTELITEN SYSTEM
GERMANY *Munich*	EDX-S EDX-C TELEX/CIRCUIT SWITCH FOR DEUTSCHES BUNDEPOST
ITALY *Milan*	INTERNATIONAL TELEGRAM FOR ITALCABLE
ITALY *Rome*	LEASED CHANNEL FOR ITALCABLE
ITALY *Rome*	INTERNATIONAL TELEGRAM FOR ITALCABLE
MALAYSIA *Kuala Lumpur*	INTERNATIONAL TELEGRAM, TELEX EXCHANGE, AFTN FOR TELECOMMUNICATIONS AUTHORITY OF MALAYSIA
MEXICO *Mexico City*	ELECTRONIC MAIL FOR NATIONAL TELECOMMUNICATIONS AUTHORITY, TELENALES
MEXICO *Mexico City*	NATIONAL TELEGRAM FOR SECRETARY OF COMMUNICATIONS AND TRANSPORT (SCT)
QATAR *Doha*	DMHS-MAILBOX, X.400, X.25, INTERNATIONAL TELEGRAM, TELEX FOR Q-TEL
SINGAPORE	INTERNATIONAL TELEGRAM, TELEX EXCHANGE, AFTN FOR SINGAPORE TELECOMS
THAILAND *Bangkok*	COMMUNICATIONS AUTHORITY OF THAILAND (CAT) FOR ELECTRONIC MAIL
THAILAND *Bangkok*	COMMUNICATIONS AUTHORITY OF THAILAND (CAT) FOR INTERNATIONAL TELEGRAM
U.S.A. *Boston, MA*	MULTI-PROTOCOL E-MAIL HUB FOR BROWN BROTHERS HARRIMAN
U.S.A. *Germantown, MD*	NETWORK CONTROL CENTER FOR A TDMA SATELLITE NETWORK FOR COMTEL
U.S.A. *Los Angeles, CA*	NETWORK CONTROL CENTER FOR A TDMA SATELLITE NETWORK FOR COMTEL
U.S.A *New York City, NY*	TELEX EXCHANGE FOR WESTERN UNION INTERNATIONAL (NOW MCI)
U.S.A *New York City, NY*	INTERNATIONAL TELEGRAM FOR WESTERN UNION INTERNATIONAL (NOW MCI)
U.S.A *New York City, NY*	LEASED CHANNEL FOR WESTERN UNION INTERNATIONAL (NOW MCI)
U.S.A *New York City, NY*	LEASED CHANNEL FOR RCA GLOBCOM

U.S.A. *Ft. Bragg, NC*	TRI-TAC AN/TYC-39
U.S.A. *Ft. Detrick, MD*	DCA OVERSEAS AUTODIN
U.S.A. *Ft. Detrick, MD*	DCA CONUS AUTODIN
U.S.A. *Ft. Gordon, GA*	TRI-TAC AN/TYC-39
U.S.A. *Ft. Hood, TX*	TRI-TAC AN/TYC-39
U.S.A. *Ft. Huachuca, AZ*	TRI-TAC AN/TYC-39
U.S.A. *Ft. Monmouth, NJ*	TRI-TAC AN/TYC-39
U.S.A. *Gentilly, OH*	DCA CONUS AUTODIN
U.S.A. *Hancock AFB, NY*	DCA CONUS AUTODIN
U.S.A. *Hawaii, HI*	DCA OVERSEAS AUTODIN
U.S.A. *Mc Dill AFB, FL*	TRI-TAC AN/TYC-39
U.S.A. *Partick AFB, FL*	TRI-TAC AN/TYC-39
U.S.A. *Robbins AFB, GA*	TRI-TAC AN/TYC-39
U.S.A. *Sacramento, CA*	DCA CONUS AUTODIN
U.S.A. *San Bernardino, CA*	DCA CONUS AUTODIN
U.S.A. *Tinker AFB, OK*	DCA CONUS AUTODIN
U.S.A *Tinker AFB, OK*	TRI-TAC AN/TYC-39
U.S.A. *Washington, DC*	DCA CONUS AUTODIN

Defense



ENGLAND	DCA OVERSEAS AUTODIN
Croughton	
GERMANY	DCA OVERSEAS AUTODIN
Pirmasens	
GERMANY	TRI-TAC AN/TYC-39
Various Bases	
GUAM	DCA OVERSEAS AUTODIN
ITALY	DCA OVERSEAS AUTODIN
Coltano	
ITALY	ITALIAN ARMY MESSAGE SWITCH
Padua	
ITALY	ITALIAN ARMY MESSAGE SWITCH
Rome	
JAPAN	DCA OVERSEAS AUTODIN
Yokota Air Base	
NETHERLANDS	ROYAL DUTCH AIR FORCE MESSAGE SWITCH
Arnhem	
NETHERLANDS	DUTCH POLICE FORCE MESSAGE SWITCH
Bilthoven	
NETHERLANDS	ROYAL DUTCH AIR FORCE MESSAGE SWITCH
Hilversum	
OKINAWA	DCA OVERSEAS AUTODIN
Camp Buckner	
PANAMA	TRI-TAC AN/TYC-39
PHILIPPINES	DCA OVERSEAS AUTODIN
Clark AFB	
SOUTH KOREA	DCA OVERSEAS AUTODIN
Camp Walker	
SOUTH KOREA	TRI-TAC AN/TYC-39
Seoul	
SOUTH VIETNAM	DCA OVERSEAS AUTODIN
Nha Trang	
SOUTH VIETNAM	DCA OVERSEAS AUTODIN
Phu Lam	
THAILAND	DCA OVERSEAS AUTODIN
Khorat Air Base	

CANADA *Montreal*	AEROPP — AFTN, HDLC, ICAO CATB, AIR-TO-GROUND
CZECHOSLOVAKIA *Prague*	AEROPP — AFTN, MET, TELEX, IATA, HDLC
ENGLAND *London*	IATA MESSAGE SWITCH FOR SITA
FRANCE *Paris*	IATA MESSAGE SWITCH FOR SITA
IRELAND *Shannon*	AEROPP — AFTN, OCEANIC CONTROL
ITALY *Rome*	AEROPP — AFTN, TELEX, HDLC
KENYA *Nairobi*	AEROPP — AFTN, FLIGHT PLAN PROCESSOR
KUWAIT *Kuwait City*	AEROPP — AFTN, REPETITIVE FLIGHT PLAN FILE
MEXICO *Mexico City*	AEROPP — AFTN, MET, IATA
NETHERLANDS *Amsterdam*	IATA MESSAGE SWITCH FOR SITA
NORWAY *Bergen*	EDX-M — AFTN MESSAGE SWITCH
PARAGUAY *Asuncion*	AEROPP — AFTN, IATA
SINGAPORE	AEROPP — AFTN, TELEX
SLOVENIA *Ljubljana*	DMHS — AFTN
SPAIN *Madrid*	AEROPP — AFTN
SWEDEN *Stockholm*	AEROPP — AFTN, TELEX
U.S.A. *Annapolis, MD*	ARINC — IATA, X.400, CORPORATE E-MAIL
U.S.A. *Atlanta, GA*	FAA NADIN I — AFTN, ADCCP, ICAO CATA & CATB, 83B3, 85A2
U.S.A. *Atlantic City, NJ*	FAA NADIN I — AFTN, ADCCP, ICAO CATA & CATB, 83B3, 85A2
U.S.A. *Kansas City, KS*	FAA WMSC (WEATHER MESSAGE SWITCHING CENTER) — AFTN, MET DATA
U.S.A. *Salt Lake City, UT*	FAA NADIN I — AFTN, ADCCP, ICAO CATA & CATB, 83B3, 85A2
VENEZUELA *Caracas*	AEROPP — AFTN, MET, FLIGHT PLAN PROCESSOR

Spanning The Globe

DATA SYSTEMS ANALYSTS, INC.

A Tradition of Service

DSA
Supporting MCI and DISA

Data Systems Analysts, Inc., (DSA) has over 34 years experience providing communications and information security consulting and engineering services to government agencies and commercial clients. DSA is providing the following information security support to MCI and DISA for the Defense Information Systems Agency (DISA) Switch/Bandwidth Manager Services CONUS (DS/BMS-C) contract:

Security Requirements Analysis & Definition:

- DISA/DoD Requirements Analysis
- Security Architecture Design Integrating Commercial-Off-the-Shelf (COTS) Security Technologies
- Strong Authentication Compliance

Network/Telecommunications Security:

- Audit Consolidation & Analysis
- 7X24 Monitoring of Security Related Events & Incident Response
- Trusted Computer Security Evaluation Criteria (TCSEC) Requirements Implementation
- Administration of Strong Authentication Mechanisms

Risk Management & Mitigation:

- Threat Assessment & Vulnerability Analysis
- Implementation of Automated Risk Assessment Tools
- Ongoing Risk Mitigation Support

Personnel & Physical Security:

- Security Awareness Training
- Personnel Clearance Administration
- Physical Security Site Surveys
- National Industrial Security Program Operating Manual (NISPOM) Requirements Implementation

Security Testing and Evaluation (ST&E):

- Test Requirements Matrix Definition
- ST&E Plans & Procedures
- Ongoing DISN Technology Lab Security Support

Certification & Accreditation (C&A) Support:

- DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Implementation
- Founded DISN Security Working Group
- Security Policy & Procedure Development
- Configuration & Change Management Support

Security Architecture Implementation & Integration:

- COTS Security Technology Integration
- DISA/DoD Security Requirements Implementation
- Configuration & Troubleshooting of COTS Security Products

New Jersey 609/665-6800 Fax 609/665-6672 • Virginia 703/591-3704 Fax 703/591-8418 • Texas 972/238-8680 Fax 972/783-9755
http://www.dsainc.com

What Can You Afford to Lose?

DSA

Information Security

Data Systems Analysts (DSA) has over 30 years experience providing communications and information security consulting and engineering services to government agencies and commercial clients. Our Information Security Engineering Team provides security planning, design, implementation, integration and conducts certification analysis for system accreditation and approval. We also offer the expertise to provide customized security services unique to client needs for data and voice communications systems. Our Security Engineering Team works with and understands private industry security standards and regulations as well as DoD and government agency regulations and standards. As a result of our extensive experience and commitment to excellence, we offer unparalleled security consulting and engineering services in the following areas:

- AIS, LAN, WAN and MLS Network Security
- Certification and Accreditation Support
- Virus Detection, Removal, and Prevention
- Information Warfare Simulation Security
- Internet and Intranet Security
- Security Test and Evaluation (ST&E) including Independent Verification and Validation (IV&V)
- Satellite Security (Terrestrial and Space Segment)
- Security Awareness and Training
- Contingency Planning and Disaster Recovery
- Red/Black Criteria Evaluation
- Electronic Mail System Policy and Procedure Development
- Standard Operating Procedures Development
- Security Policy and Procedures Development
- Physical and Personnel Security Requirements Analysis
- Private Telephone Branch Exchange (PBX) Security
- X.400 and X.500 Security Analysis

We have provided security engineering and consulting services to various Department of Defense and Military service agencies and commercial clients. Most recently, with an international telecommunications company, we are participating in a $400 million contract to provide information security consulting and engineering services to the Defense Information Systems Agency (DISA) for the Defense Information System Network (DISN). Other projects include, the Defense Message System (DMS), the On-Site Inspection Agency (OSIA), the Automatic Digital Network (AUTODIN) and the Federal Aviation Administration (FAA).

We also provide information security services to major commercial clients including financial organizations, enhancing their overall operational and technical security. Additionally, for an international telecommunications company, our Security Engineering Team has provided both terrestrial and space segment information security solutions for a large scale commercial satellite network.

New Jersey 609/665-6800 Fax 609/665-6672 • Virginia 703/591-3704 Fax 703/591-8418 • Texas 972/238-8680 Fax 972/783-9755
http://www.dsainc.com

DSA and Aeronautical Messaging

Aeronautical message handling requires the highest performance and reliability standards for software and systems. DSA has been pivotal in the development of some of the most impressive aeronautical systems in the world and has many significant "firsts" to its credit. These include:

- the design and implementation of what many consider the world's first packet switching network for the Société Internationale des Télécommunications Aeronautiques (SITA) in the late 60s,
- software for the first fully automated AFTN Centre for the FAA under contract to) North American Philips (NAP),
- replacing the above software in the NADIN I message network including the first CIDIN links (panel 8) under contract to NAP,
- the first commercially available AFTN/ATN gateway as part of its **A•MHS** (Aeronautical Message Handling System) product.

DSA has developed a wide range of aeronautical systems with unique combinations of capabilities and custom features that have been installed in many countries spread over four continents as the following list shows.

Countries where aeronautical software or systems developed by DSA have been deployed:

- Canada
- Czechoslovakia
- France
- Germany
- Indonesia
- Ireland
- Italy
- Kenya
- Kuwait
- Morocco
- Malaysia
- Mexico
- Netherlands
- Norway
- Paraguay
- Singapore
- Slovenia
- Spain
- Sweden
- United Kingdom
- United States of America
- Venezuela

DSA now offers its **A•MHS**, a scaleable message product with true client/server architecture for use as a message switch, a concentrator, or a gateway.

New Jersey 609/665-6800 Fax 609/665-6672 • Virginia 703/591-3704 Fax 703/591-8418 • Texas 214/238-8680 Fax 214/783-9755
info@dsainc.com

C^4I
FOR THE WARRIOR

GCCS
GLOBAL COMMAND & CONTROL SYSTEM

FROM CONCEPT TO REALITY

"The history of command can thus be understood in terms of a race between the demand for information and the ability of command systems to meet it."

Martin Van Creveld
Command in War

"What the Warrior Needs: A fused real time, true representation of the Warrior's battle space—an ability to order, respond and coordinate horizontally and vertically to the degree necessary to prosecute his mission in that battle space..."

Richard C. Macke
Vice Admiral, USN
C4I for the Warrior
12 June 1992

12 June 1994

The C4I for the Warrior concept is committed to the challenge of meeting the warrior's quest for information needed to achieve victory for any mission, at any time and at any place. The C4I for the Warrior concept is the vision and a roadmap for providing such information support to the joint warfighter.

Activities necessary to achieve this vision have already been set in motion, and significant progress is being made. A solid foundation for progress is in place in national military strategy, DOD interoperability policy, new C4I systems acquisition requirements, and joint warfighting doctrine. The groundwork is clearly established to resolve future interoperability issues and provide new capabilities to the warrior to acquire the necessary knowledge needed for victory in today's information-based world. Victory has been declared in the first phase of the march!

A Midterm Phase goal of producing a global C4I system capable of generating and delivering the fused information needed for tactical command decisions is at hand. The Global Command and Control System (GCCS) is evolving to be the joint C4 system of C4 systems, interoperable through common paths and common switches, and for the first time providing the joint forces commander with a true picture of the battle space as earlier envisioned in the C4I for the Warrior concept.

The brochure focuses on the GCCS, the support it is receiving from related C4I for the Warrior activities, and the progress being made in transforming the C4I for the Warrior vision into reality for today's and future warriors.

JOHN M. SHALIKASHVILI
Chairman
of the Joint Chiefs of Staff

PREPARING FOR THE MARCH: SET THE COURSE

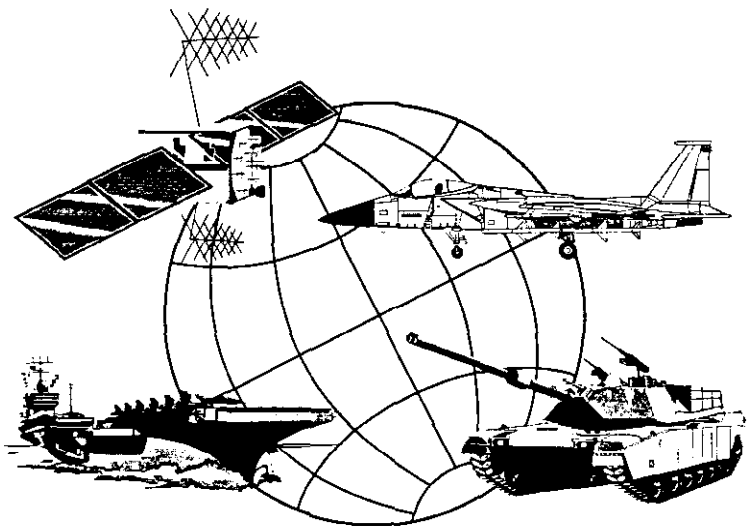
The C4I for the Warrior concept established unity of effort and is providing the necessary information for warfighters to win on today's and future battlefields.

The common vision of the C4I for the Warrior concept is to create a broadly connected joint system of joint systems that provides total battle space information to the warrior. This C4I information infrastructure provides seamless connectivity for the warrior to "plug in" and obtain the information, offensive and defensive, needed to carry out any mission, at any time and at any place.

The problems in conducting joint operations because of noninteroperable C4I systems are well known. The great need for interoperability among Service and combatant command (CINC) C2 systems is well established. Organizational and unit integrity, supported by dedicated networks and systems, is essential for the joint force commanders to conduct effective combat operations. Joint operations involving multiple land, sea, and air units in adaptive joint force structures increasingly require joint networks and joint systems that are fully interoperable horizontally across air, sea, space, and ground environments.

The commitment by the Joint Staff, combatant commands, Services, and Defense agencies to the vision of total C4I joint interoperability provides a measure of stability and assurance at a time when the warrior's job requires a quick reaction and adaptive response to uncertain and dangerous situations.

In the C4I for the Warrior concept **interoperability** is defined as the capability of people, organizations and equipment to operate effectively and efficiently together for successful mission accomplishment. This definition has not changed.

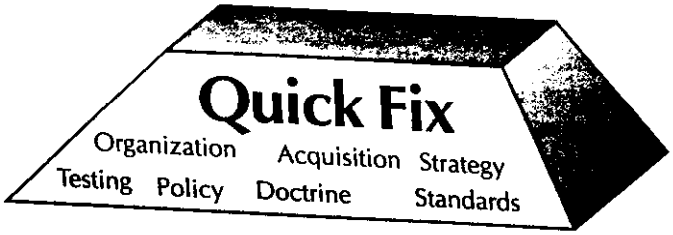


"We are looking for the 80 percent solutions as we work toward the goal of complete interoperability."

Albert J. Edmonds
Lieutenant General, USAF
Director, Command, Control, Communications, and Computer Systems, J6
Joint Staff

The C4I for the Warrior concept is a vision with an accompanying roadmap for realizing the concept. In the past 2 years it has received enthusiastic support, both as a much needed vision and as a pragmatic roadmap to accomplish the vision. The assignment to turn the concept's vision into reality has been a well accepted team endeavor. The job, however, is not finished. ***The J6 strategy for finishing the job is to go with "winners," as measured by the actual warfighter.*** The roadmap must be flexible enough to accommodate changing warrior requirements, advancing technology, and ever decreasing C4I budgets.

QUICK FIX VICTORIES



The Quick Fix Phase paved a new way of doing business and introduced interoperability improvements into the field.

The initial C4I for the Warrior roadmap comprised three phases:

- Quick Fix Phase.
- Midterm Phase.
- Objective Phase.

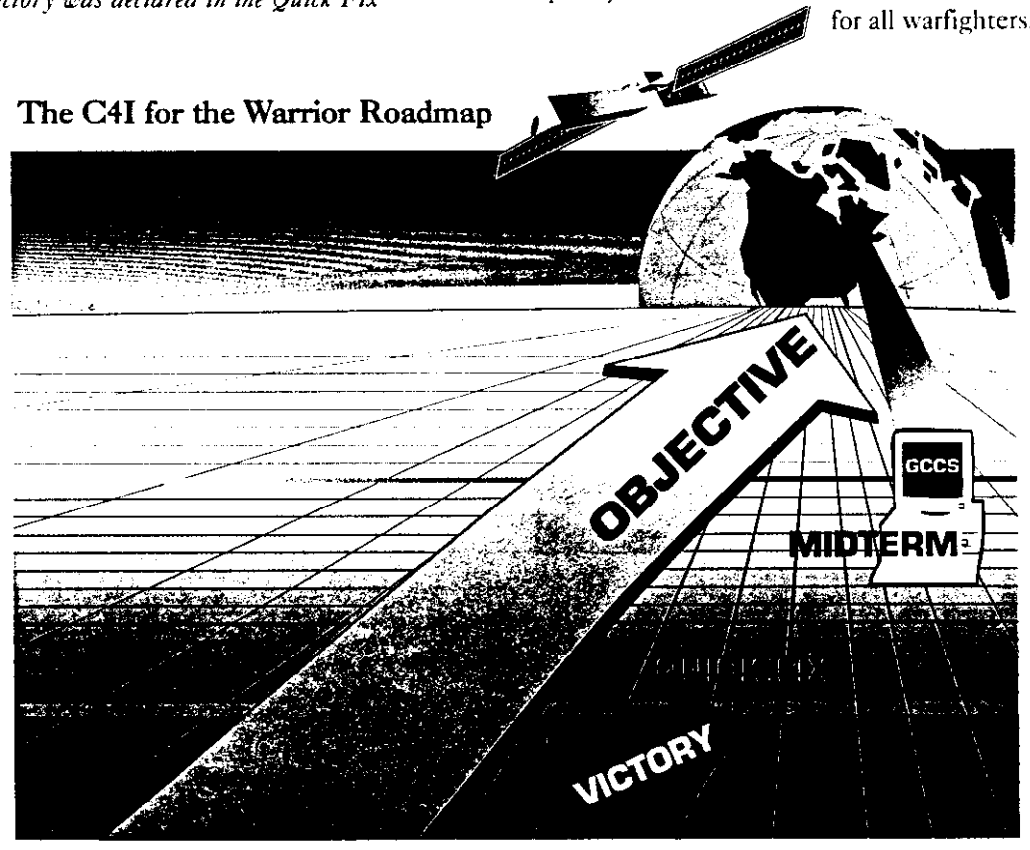
These have not changed.

The **Quick Fix Phase** *included promulgation of the new C4I for the Warrior concept's paradigm, new policy and doctrine implementers and interoperability design and engineering projects that could be completed quickly and that would result in near-term, high leverage interoperability improvements. These activities have been completed successfully and victory was declared in the Quick Fix Phase in 1993.*

The C4I for the Warrior concept has a solid foundation that is now firmly established in strategy, policy, acquisition, and doctrine. This foundation will ensure that the warrior's requirements continue to drive the quest for information and interoperability.

The objective is to improve the quality and utility of military needed information while reducing the annual cost of military operations without losing sight of the warfighter's perspective. The plan for implementing the strategy is to use a migration approach, achieve improved functionality and cross-functional integration based on accelerated process improvement reviews and assessments, and incorporate interoperability, technical integration, military standard data, and integrated data bases to provide higher quality and lower cost information technology services for all warfighters.

The C4I for the Warrior Roadmap



PROOFS OF CONCEPT

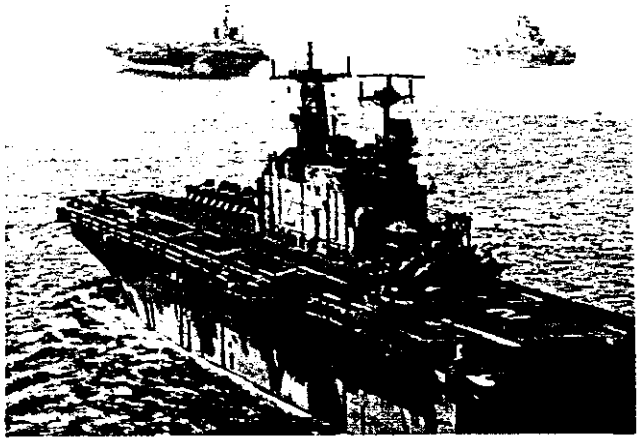
The Joint Universal Data Interpreter (JUDI) was a Quick Fix interoperability initiative. JUDI found a quick technical solution to data format incompatibility and demonstrated that existing systems could be made to interoperate without major modifications. The JUDI approach showed that diverse systems could be integrated effectively and paved the way for the GCCS migration system approach that is now in progress.

The Services have provided their support to the C4I for the Warrior concept through action:

- *The Army's Enterprise Strategy sets forth 10 principles that support US Army warfighters into the 21st century and synchronize Army programs with the Joint Staff's C4I for the Warrior concept.*

"We will rely on America's dynamic new base of available technologies to tailor our fighting force to tomorrow's battlefield."

US ARMY, *ENTERPRISE*



- *The Navy's Copernicus architecture establishes a framework for restructuring its C4I strategy. It also addresses the challenges of developing new technologies to integrate sensors, facilitate tactical decisionmaking, and solve communications capacity problems. It is a vision for moving into the 21st century.*

"We have crossed the threshold of the Information Age—an age in which the pace of progress in all fields of human knowledge is hastening forward. The impact of this revolution will be experienced worldwide, presenting both risks and opportunities."

US NAVY, *COPERNICUS*

- The Air Force's HORIZON strategy provides a fundamental reference for optimizing C4I capabilities from the present day into the 21st century. Its goal is to evolve present and proposed C4I capabilities into an integrated, interoperable, global network—an infosphere—that meets Air Force, joint, and DOD requirements.

"It is vital that the C4I capability supporting the Air Force in this era of dynamic change not merely keep pace; the C4I capability must be moved ahead, out in front of the waves of change."

US AIR FORCE, *HORIZON*

- The Marine Corps' commitment to provide a unique warfighting capability that supports the National Military Strategy is predicated on maintaining integrated Marine Air Ground Task Forces (MAGTFs). A fundamental component of this capability is modernized, integrated C4I systems that support the warfighter. The Marine Corps' MAGTF C4I strategy embraces the principles of the C4I for the Warrior concept of providing the required information to the warfighter.

"The measure of command and control effectiveness is simple: either our command and control works faster than the enemy's decision and execution cycle or the enemy will own our command and control."

Fleet Marine Force Manual (FMFM) 3, Command and Control

NEW WAY OF DOING BUSINESS

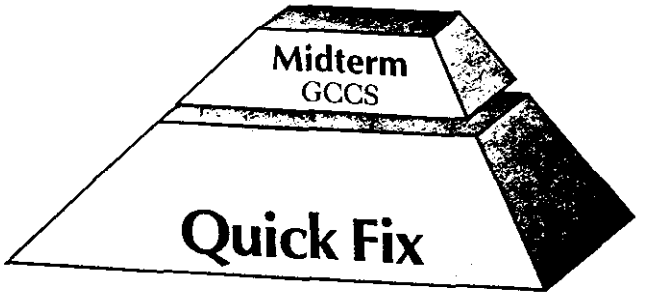
The new way of doing business involves the entire C4I community and streamlines the organizations and processes concerned with specifying, testing and acquiring C4I systems. The Joint Requirements Oversight Council (JROC), a reorganized Military Communications-Electronics Board (MCEB), the Center for Standards within the Defense Information Systems Agency (DISA), and parallel Service and Defense agency organizations are focusing on more effective and efficient C4I, using the C4I for the Warrior concept's paradigm as the model for matching resources and plans against requirements. In addition to real world opportunities such as Operations DESERT SHIELD and DESERT STORM, joint exercises and operational demonstrations provide realistic conditions for testing new ideas and capabilities.

The Joint Warrior Interoperability Demonstration (JWID) 94 will be the fifth in a series of operational demonstrations to show what works and what does not before major C4I acquisition commitments are made. Seventy DOD and vendor demonstrations are currently proposed in the categories of battle space management, collaborative planning, smart push and warrior pull, and interoperability of joint communications and networks.

Acquisition streamlining is a key element in the new way of doing business. Standardization, use of commercial off-the-shelf (COTS) hardware and software, and parallel development activities, such as bringing the testers and users into the development process in the early stages, shortens development time and reduces costs.

GCCS will profit from the new way of doing business. It is not a GRAND DESIGN effort, and it is not a 100-percent solution. It is an initiative that goes a long way toward eliminating inflexible stovepipe systems and expensive duplication. And it is doing it today.

THE MARCH



The Midterm Phase demonstrates the initial operational capabilities of the GCCS "system of systems" and sets in motion the process for selecting and implementing "best of breed" migration systems and technology insertion projects.

GCCS responds to the warrior's need for a fused, real-time true picture of the battle space and the need for the ability to order, respond, and coordinate vertically and horizontally to the degree necessary to prosecute the mission in the battle space.

"As always, the perspective of the warfighter must be maintained throughout the selection process."

Honorable Emmett Paige, Jr.
Assistant Secretary of Defense
(Command, Control,
Communications & Intelligence)
20 December 1993

The **Midterm Phase** in the form of GCCS is marching toward the C4I for the Warrior concept's vision of an objective. The interoperability targets of this phase are being realized through "right sizing," prototyping, tactical system enhancements, and migration of "best of breed" Service and Defense agency existing legacy systems into GCCS. Achievements include:

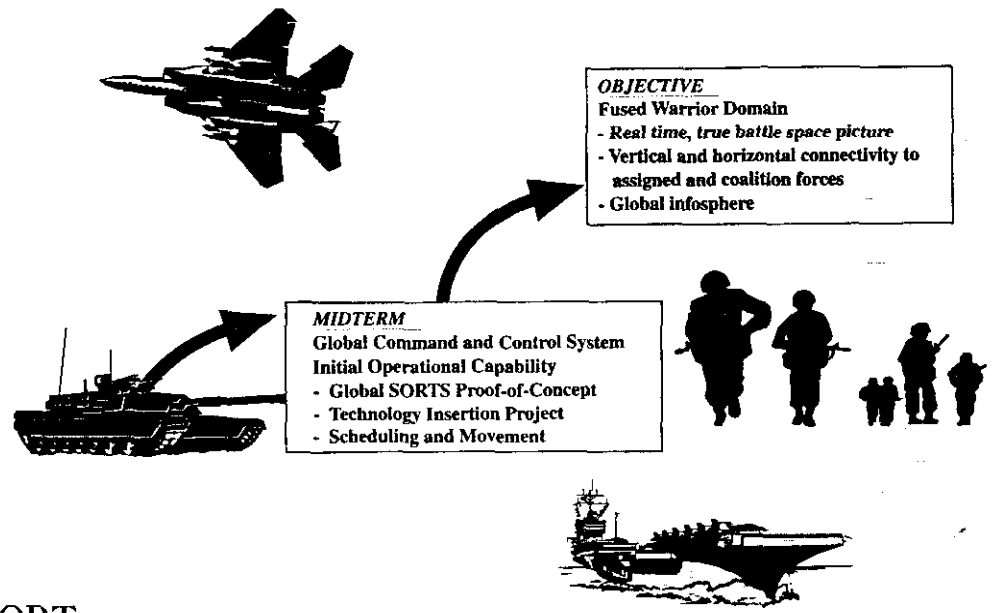
- System development and modernization programs, such as GCCS, are using new, streamlined, evolving selection and certification procedures that respond directly to the warfighters' requirements.
- Fixed, transportable, and tactical communications are rapidly achieving a high degree of applications standardization and levels of interconnectivity capable of supporting joint or multinational operations, independent of time, space, and sponsorship considerations.
- Unique military standards and devices are giving way to commercial standards.
- The components of the global C4I infrastructure supporting joint operations continue to evolve toward a single interoperable system, GCCS.

MIGRATION:
The systematic selection, introduction, and assimilation of existing system software functionalities into GCCS core functions, operating in the GCCS common operating environment.

LEGACY SYSTEM:
A legacy system consists of the older hardware or software components of an existing system that are replaced or modified by newer implementations.

GCCS COMMON OPERATING ENVIRONMENT (COE):
Computer applications programs that support the fundamental processes involved in planning and conducting military operations.

GCCS: The Bridge to the C4I for the Warrior Objective



C4I SUPPORT FOR THE WARFIGHTER TODAY: THE NEED FOR GCCS

All military C4I systems have one job—to support the warfighter. GCCS provides the best opportunity for establishing an effective, efficient bridge to the C4I for the Warrior concept's objective. It incorporates the core planning and assessment functions identified and needed by the commanders of combatant commands (CINCs) and their joint force commanders, and it meets the readiness support requirements of the Services while accommodating their unique regional and functional information requirements.

Too many stovepipe systems and too much duplication exist in the C4I arena. GCCS provides an effective baseline vehicle for implementing the much needed C4I system consolidation and migration strategy.

GCCS CORE FUNCTIONALITY:
The GCCS core consists of the basic functions required by a warfighter to plan, execute, and manage military operations. These basic functions are satisfied by selecting the "best of breed" applications from existing C2 systems. This process ensures interoperability, minimizes training requirements, and allows efficient use of limited defense resources.

RIGHT SIZING:
A conceptual tenet that has allowed us to transition technical potential to reality. Right sizing is the matching of performance, schedule, and cost to the objective.

The migration process selects from among all candidate systems those that are best at the jobs they do in support of the warfighter and migrates those capabilities into GCCS. The CINCs have identified the core functions as:

- Crisis Planning.
- Force Deployment.
- Force Employment.
- Force Status.
- Logistics.
- Air Operations.
- Fire Support.
- Intelligence.
- Personnel.
- Position.
- Narrative Information.

UNDERSTANDABLE INFORMATION

Interoperability is not limited to information sharing. The way in which information is presented is as important as its availability.

Old Method

- Not user friendly
- Six week school to train
- Expensive to change code

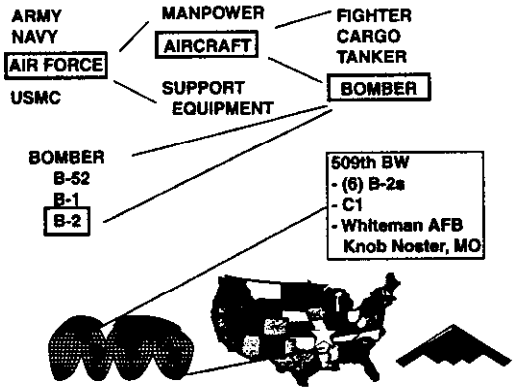
```
SELECT t0.ANAME,t1.MEQPT
       t1.MEPSA,t1.MEORN
       t1.MEORD
FROM GEOT t0,MELLONC
WHERE t1.UIC(+)=t0.UIC
 AND (t0.UIC + 'M368856')
```

- Output not easily readable

ANAME	MEQPT
1ST BN 2D MAR	105 HOW TD
1ST BN 2D MAR	AAVC7A1
1ST BN 2D MAR	AAVP7A1
1ST BN 2D MAR	LAV-25
1ST BN 2D MAR	LAAV-25AT
1ST BN 2D MAR	M101A

New Method

- Menu/Mouse driven
- Train user in hours at home station
- Graphical displays



When you install software for your home or office computer, can you afford to go away for 6 weeks to learn how to use it? Neither can the warrior.

BRINGING C4I SUPPORT TO THE WARFIGHTER: GCCS ACTIONS AND ACCOMPLISHMENTS

GCCS is building on the C4I for the Warrior concept's foundation and is being implemented through an evolutionary strategy of right sizing and migration. **GCCS will be no larger or smaller than actually needed by the warfighter.** It is not a grand design system. GCCS features and functionalities will be selected from among existing C4I systems, and "best of breed" characteristics will be integrated into a common operating environment. As examples, consolidation of numerous force readiness status systems into a single system is taking place and action is in progress toward a single weather system that will serve both the Navy and the Air Force. The end results will be the elimination of duplication and increased interoperability among the joint C4I community.

GCCS will reengineer and migrate only the WWMCCS applications the warfighters require. Migrating these functions to GCCS in rapid succession will provide a solid, self-sustainable core and will allow effective use of a unified data base. It is expected that as warfighters draw increasingly from GCCS, their dependence on other systems will diminish, and eventually the legacy systems will no longer be needed. Warfighter selected WWMCCS functions will migrate to GCCS within the next 2 years. Unique systems will continue to be operated and supported only if their functionality does not exist on GCCS and a strong operational requirement is provided.

To ensure a successful GCCS implementation:

- Software will undergo thorough laboratory testing before release to the field.
- Current WWMCCS capabilities will be maintained until warfighters are satisfied with GCCS functionality.

"Any military—like any company or corporation—has to perform at least four key functions with respect to knowledge. It must acquire, process, distribute, and protect information, while selectively denying or distributing it to its adversaries and/or allies."

Alvin and Heidi Toffler
War and Anti-War

GCCS TRAINING

GCCS training will be synchronized with GCCS fielding. Quality training is an essential step in meeting the established goal for shutdown of WWMCCS hosts and migration of essential WWMCCS capabilities to GCCS.

As a key first step toward meeting this goal, a GCCS Single Service Training Manager (SSTM) is being established. A training concept is being developed and WWMCCS SSTMs are building the framework for GCCS functional and technical training.

GCCS system administration training has already been scheduled and the GCCS COE course will be available in July 1994. The COE course will provide training on the infrastructure of GCCS, which provides platform services and support applications such as e-mail, word processing, conferencing, and spreadsheets. In the interim, contractor training is being provided during fielding.

The composition and roles of GCCS on-site teams are being defined, and associated training requirements are being addressed.

GCCS is being fielded and tested as improvements take place. *Active participation in the process by the combatant commands and Services is the key to success. GCCS is a warfighter-driven system. It is the baseline system for command and control and its vastly improved capabilities, in prototype versions, have already proved their worth in the field.*

GCCS reengineering and development will be in versions. The first and ongoing version is the Proof-of-Concept. The goal for the Proof-of-Concept version is to form the GCCS core, which initially will be made up of a variety of functionalities such as:

- Tactical Displays.
- Message Handling.
- Air Tasking Order (ATO) Dissemination.
- Readiness Status.

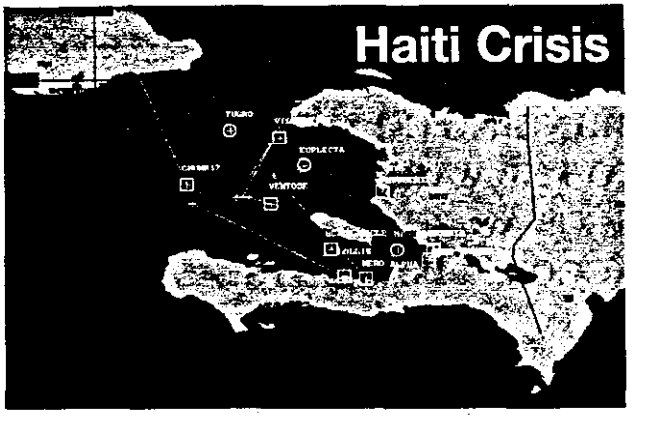
The core will grow as GCCS is implemented.

In June 1993, the GCCS first stage Proof-of-Concept version was demonstrated to senior representatives from the combatant commands, Services, and Defense agencies. The National Military Command Center (NMCC), US Atlantic Command (USACOM), US Special Operations Command (USSOCOM), and US Central Command (USCENTCOM) were linked and successfully used:

- The residual Status of Resources and Training System (SORTS) application and data.
- A new user-designed interface.
- Standard Defense Mapping Agency maps and charts.
- COTS equipment, software design and support tools, and operating system.

In early October 1993, a crisis action team (CAT) was activated in the USACOM Joint Operations Center (JOC) to carry out Haitian combined operations planning activities among national security, national defense, and allied decisionmakers.

Coincidentally, a GCCS proof-of-concept version was installed shortly after the CAT was activated. It was placed into operation immediately and was met with universal acceptance and acclaim. The GCCS continues to be used by USACOM to view the tactical situation in near-real-time and to monitor the readiness and deployment status of the joint task force.



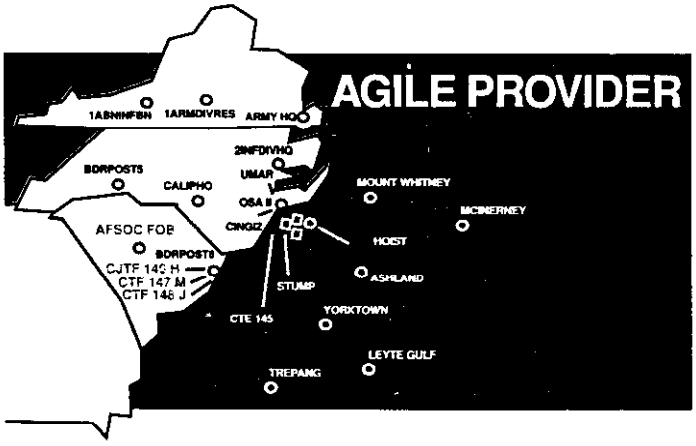
Both the CINC and CJTF were able to simultaneously view a collective laydown of red and blue ground, seaborne and airborne forces operating in the joint operating area (JOA) on a single C2 screen.

Graphical displays replaced text and the CINC had clear, easily readable readiness data as well as imagery and connectivity to his four components—all at his fingertips.

In February 1994, the GCCS prototype implementation between USACOM and the US Transportation Command (USTRANSCOM) was established. This accomplishment directly links a warfighting CINC with the information available to a critical supporting CINC and provides a significant opportunity to test the C4I for the Warrior concept's information "pull" and "push" tenets.

In May 1994, a postexercise report from USACOM stated that GCCS "met or exceeded all exercise objectives, and provided significant increase in C2 function to USACOM." During AGILE PROVIDER 94, the capability of GCCS to provide a common picture of the battle space was tested as an objective of USACOM's joint field training exercise, designed to train forces in the planning and conduct of joint combat operations.

Version 2.0 of GCCS will be introduced in late 1994. GCCS will be implemented at each CINC, and testing of the Scheduling and Movement functionality will begin. A foreseeable challenge is converting the Joint Operations Planning and Execution System (JOPES) from its current mainframe environment into one more usable by GCCS.



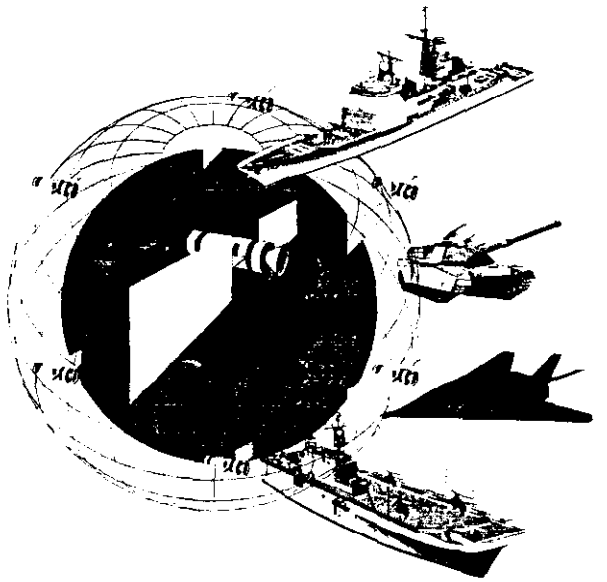
COMMON PIPES AND COMMON SWITCHES

The Defense Information Systems Network (DISN) and ongoing efforts for providing common tactical switches will provide much of the enabling connectivity to bring the GCCS pieces together in reaching the C4I for the Warrior concept's objective.

DISN is the DOD consolidated worldwide enterprise level telecommunication infrastructure that provides the end-to-end information transfer network for supporting military operations. It is transparent to its users and is responsive to national and security needs under all conditions. DISN provides long haul end-to-end common user and dedicated telephone, data, and video service.

DISN will interoperate with the Federal Telephone System (FTS 2000), which will provide the following services:

- Switched voice service for transmission of voice and data. This service allows the fast transfer of information from host and personal computers, facsimile machines, and other equipment when the traffic is not sufficient to justify a dedicated line.
- Video transmission service for compressed video and full motion teleconferencing.
- Packet switched service for data transmission in a packet format.
- Dedicated transmission service for voice point-to-point line service.
- Switched digital integrated service for the integrated transmission of services using T-1 or the Integrated Services Digital Network (ISDN).



"The joint campaign should fully exploit the information differential, that is, the superior access to and ability to effectively employ information on the strategic, operational and tactical situation which advanced US technologies provide our forces."

JOINT PUB 1

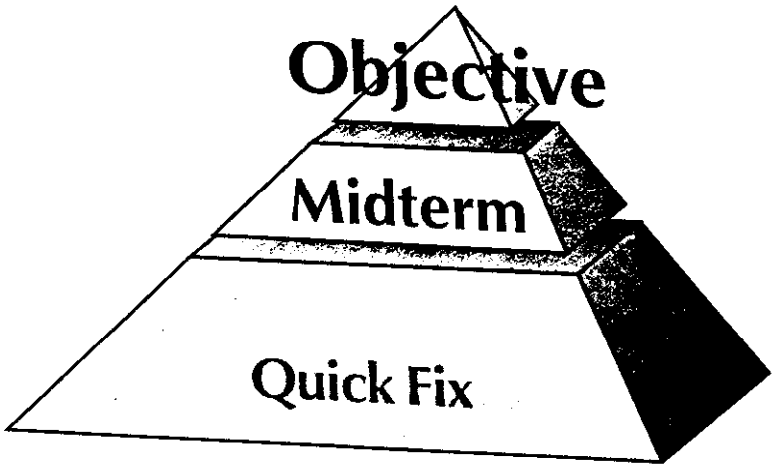
Plans are underway for the migration of software baselines of eight different switches, which currently use different routing algorithms and data rates into a single enhanced software baseline package. Operation of tactical switching networks will be simplified and maintenance will be easier. The baseline will be used as a conduit for the migration of switching networks toward COTS products, thereby producing a larger, integrated network of common switches.

In late 1993, the space-based Global Positioning System (GPS) constellation became operational and is now capable of providing 24-hour worldwide, all-weather, passive, three-dimensional position, velocity and timing data to US and allied military forces. GPS will be integrated into virtually every platform and weapon system by 2000. The result will be enhanced situational awareness information, available to the warfighter as a component of GCCS.

An adversary's C4I system is an attractive military target. Conversely C4I Protect is important to sucessful military operations. In addition to providing a rapid flow of accurate information, the C4I for the Warrior concept must establish C4I systems resilient to actions that degrade the system components—people, procedures, communications paths, switches, hardware and software, and the information itself. Under the provisions of the J3 Directorate's C2 warfare concept, the J6 Directorate will protect the availability and integrity of information needed by the warrior. The C4I technology revolution, the information explosion, commercialization of DOD communications paths and switches, use of COTS products, and decreased frequency spectrum availability are considerations that impact the availability of information as it applies to all traditional warfighting disciplines. In response, C4I Protect measures are integral to the C4I for the Warrior concept's "march."

GCCS implementations are going to meet the C4I requirements of the National Command Authorities, CINCs, joint force commanders, Services, and supporting commands. GCCS will also provide information processing technologies required for the CINCs to develop and execute those plans and contingencies that support our national military strategy.

THE WARRIOR'S SOLUTION: ONE COMMON SYSTEM



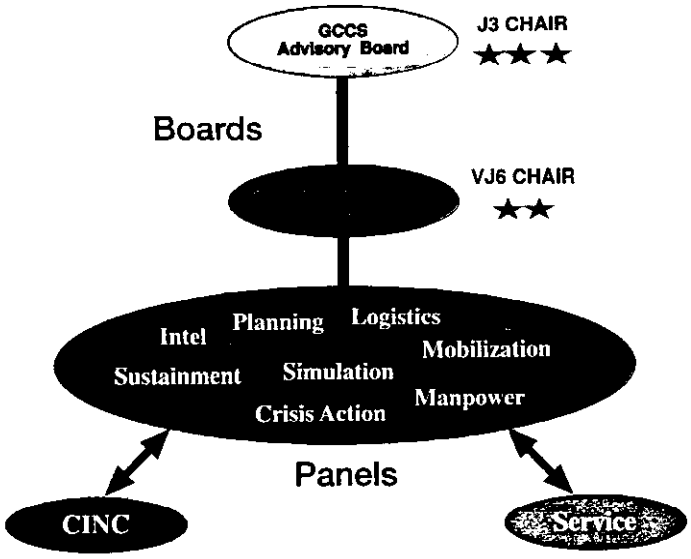
GCCS guides the march toward the vision.

GCCS's newest Proof of Concept implementation has been demonstrated successfully. A documented concept of operations is being developed and efforts continue uninterrupted to realize the vision of a unified, interoperable, and global C2 system. The success of GCCS implementation is related directly to the involvement of warfighters as well as support from the Services and Defense agencies, particularly since the GCCS implementation strategy relies heavily on reuse of existing software and warrior input.

GCCS is not a hardware acquisition project and will be hardware independent. It will have a standardized COE and provide core applications to achieve warrior-specified performance needs and interoperability objectives. For example, GCCS will be UNIX-based. A comprehensive approved products list is being promulgated to allow warfighters to acquire hardware that meets GCCS technical interface specifications. GCCS will evaluate and select for reuse applications from candidate systems recommended by the Services and Defense agencies, within the goals established for functional capabilities, performance, interoperability, and cost. The selection process is an objective, participatory evolution that will result in the migration of software applications certified by previous warfighters and endorsed by current warfighters. The process will be subject to approval by the J3 and the J6, and reviewed periodically by the Assistant Secretary of Defense (Command, Control, Communications and Intelligence).

> **"I will support only one [Joint] Command and Control System."**
>
> General John Shalikashvili
> Chairman of the
> Joint Chiefs of Staff

THE C4I FOR THE WARRIOR VISION



GCCS Management Structure

*The **Objective Phase** uses continually advancing technologies and experience gained during earlier and ongoing initiatives to achieve optimized C4I support for the warrior.*

The C4I for the Warrior concept has a vision that includes:

- A GCCS foundation leading to a C4I for the Warrior global national military security C4I infrastructure.
- An integrated battle space defense information infrastructure that embodies the mechanisms for meeting the warrior's quest for the information needed to achieve victory.
- Highly mobile tactical C4I nodes which are integral to the warrior's functional assignment and which will provide all information needed to formulate the knowledge necessary for victory.

Effective management of the GCCS evolution, including development, implementation, security, operation, and maintenance, is essential to ensure that the system is responsive to the needs of the warfighter. The Chairman of the Joint Chiefs of Staff is ultimately responsible for policy guidance and oversight of GCCS. The GCCS Advisory Board, composed of representatives from the Joint Staff directorates, Services, and DISA, is responsible for implementation. A separate GCCS division (J6V) has been established in the J6 Directorate to fulfill the Joint Staff's system sponsorship and implementation responsibilities, which include requirements review and planning, funding allocation, and DISA project management liaison.

The C4I for the Warrior concept is becoming reality. GCCS is real, as are other C4I initiatives that were not addressed in detail in this brochure. Work continues in interoperability engineering, standardization, and information technology insertion. Standardization of data elements and interface protocols, multimedia systems with multilevel security features, and software tools that are easier to use, faster, and better tailored to the functions of the user are needs that are recognized.

"We are not building a perfect system. We're building one that meets the warrior's needs."

Albert J. Edmonds
Lieutenant General, USAF

GCCS will operate on an evolving joint network of joint networks for all worldwide military and government communications traffic with interconnection to the global information infrastructure. GCCS and related initiatives will fulfill the vision of the Objective Phase of the C4I for the Warrior concept of fused real-time situational awareness knowledge in all of its dimensions, fully integrated horizontally and vertically.

The promise of the 21st century depends upon the commitment to the quest for information, to the knowledge that it brings, and to the understanding of how best to use that knowledge in support of the warrior's march.

"Committed, Focused, and Needed"

C4I FOR THE WARRIOR

The C4I for the Warrior Concept

Architecture and Integration Division (J6I)
J6, Joint Staff
The Pentagon
Washington, D.C. 20318-6000
(703) 614-7004, DSN 224-7004
FAX (703) 697-6610, DSN 227-6610

Global Command and Control System Division (J6V)
J6, Joint Staff
The Pentagon
Washington, D.C. 20318-6000
(703) 614-7774, DSN 227-7774
FAX (703) 697-4937, DSN 224-4937

The C4I for the Warrior concept is the J-6 Directorate's commitment to the challenge of meeting the warrior's quest for information—information needed to achieve victory for any mission, at any time and at any place. The Global Command and Control System (GCCS) is a bold initiative—a much needed approach to give the warrior a true real-time secure picture of the battle space.

Albert J. Edmonds
Lieutenant General, USAF