

Chapter 10

Applying the Information Capabilities Framework at HQ, USPACOM

By
Randall C. Cieslak, CIO, US Pacific Command

10.1 INTRODUCTION

The Information Capabilities Framework (ICF) provides a requirement grid which systems and efforts must overlay to portray their contribution to end-to-end capability. This is markedly different than process diagrams that lead to systems for point (stovepiped) solutions. The ICF works in conjunction with the C4ISR Architecture Framework that calls for operational, system, and technical views of the architecture. The ICF organizes and relates efforts as well as systems. It supports the evolution of architectures over time and provides the structure needed for change management. The ICF is based upon the combination of the Global Information Grid (GIG), the Defense Information Infrastructure (DII) and a standard process organization model.

Intended use of the framework:

- Categorize projects, programs, and initiatives to illustrate how resources are being allocated to information infrastructure areas. This will allow us to identify dependencies, priorities, efficiencies, and opportunities to leverage resources.
- Illustrate the status of information infrastructure over the enterprise, including how various system events affect other parts of the infrastructure.

- Organize projects, programs and initiatives to synchronize efforts and identify essential information capability elements that are not being covered.
- Serve as a common frame of reference to communicate C4ISR and Information Technology (IT) requirements and limitations between the IT providers (e.g., J6 staff) and the operational customers.

10.2 EXECUTIVE SUMMARY

The Information Capabilities Framework (ICF) provides a grid of requirements upon which systems and efforts must overlay to portray their contribution to end-to-end capability. This is markedly different than process diagrams that lead to independent systems to achieve stovepiped solutions. The ICF provides the catalyst that allows the traditional C4ISR Architecture Framework to support the evolution of improved operational, system and technical architectures over time, through guiding the integration of many diverse efforts created independently.

The ICF was created by combining the common elements of the Global Information Grid (GIG), the Defense Information Infrastructure (DII) and a process model adapted from the U.S. Naval Facilities Engineering Command (NAVFAC). These models are adapted to characterize all aspects of information capability, from network operations through knowledge management and process improvement.

System administrators, technicians, operational users, and program managers will use this frame of reference to determine their roles in providing end-to-end information capability. Figure 1 illustrates this relationship. The most visible application of this may be in describing the status of the information infrastructure to executive leadership and other top decision-makers.

Figure 2 illustrates a high level view of the ICF with one layer expanded to highlight how users interface with the information infrastructure through common, operational, and operational support applications. Figure 3 illustrates how the ICF can provide a consistent and coherent status of the Pacific Theater Information Infrastructure.

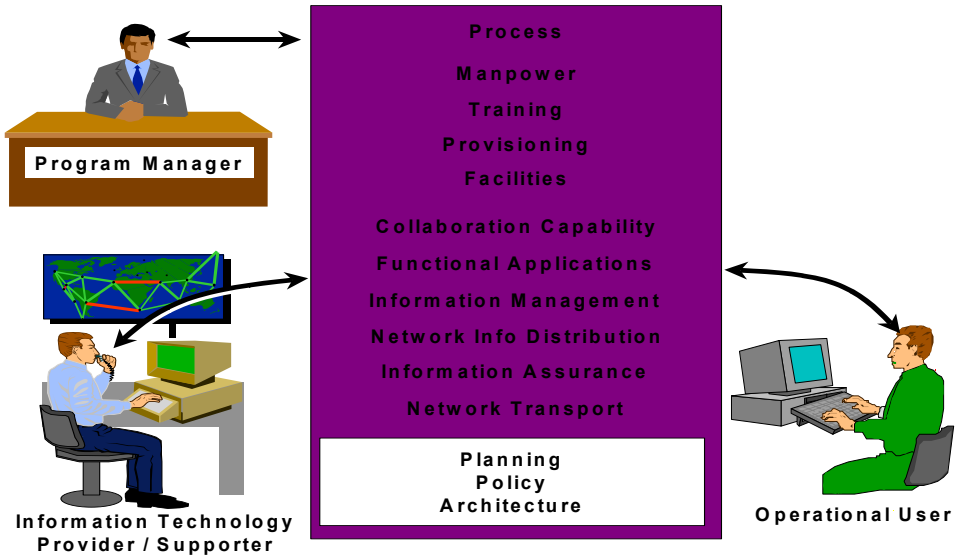


Figure 10-1. Using The ICF To Bridge The Understanding Gap Between Information Professionals, Operational Users and Program Managers

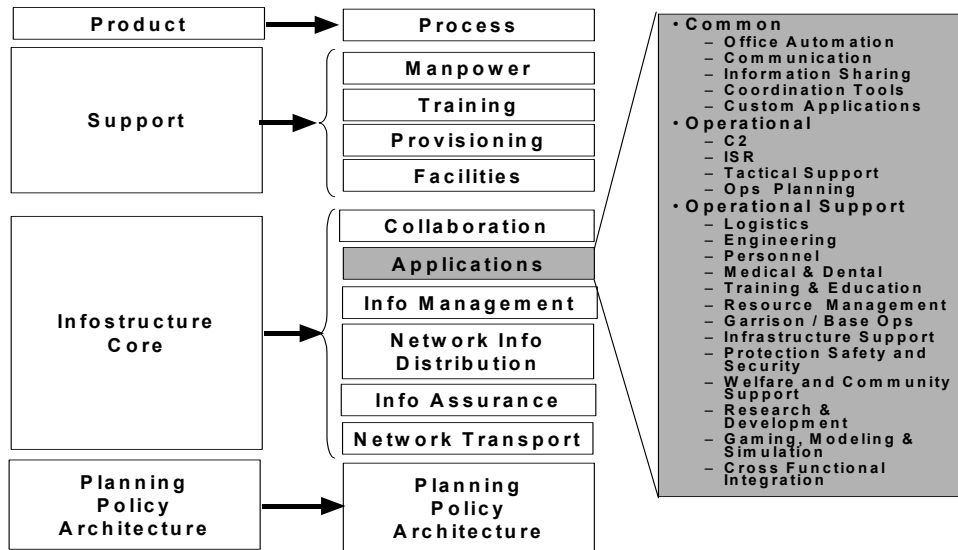


Figure 10-2. Information Capabilities Framework High-Level Organization

Information Infrastructure Status for DATE	HQ											SPEC INT					
	NCA	USCP	PACFLT	PACAF	ARPAC	MARFOR	SOPAC	USFK	USFJ	ALCOM	JJATF WEST	JTF FA	JTF CG	COMP PROVIDED	USGET	JRAC	CINC TRAVEL
Collaboration Capability																	
Conferencing																	
Communication																	
Info Sharing																	
Coordination																	
Applications																	
Web Apps																	
Messaging																	
GCCS																	
GCSS																	
Video Network Services																	
DVS																	
Other VTC																	
Voice Network Services																	
Coml. Voice																	
Radio Voice																	
DSN																	
DRSN																	
Data Network Services																	
INTERNET																	
NIPRNET																	
SIPRNET																	
JWICS																	
Info System Security																	
InfoSec																	
Network Transport																	
Mobile Radio																	
MILSATCOM																	
Coml. SATCOM																	
Wide Area Net																	

Radio Voice Transceiver Power Supply Failure. ETR 1300Z
Collaboration capability limited to HQ only.

Figure 10-3. Information Capabilities Framework High-Level Depiction of Theater Information Infrastructure Status

A robust information infrastructure is required to enable USPACOM forces to establish and maintain information superiority and therefore support USCINCPAC's mission, vision and objectives. The ICF will enable USCINCPAC's holistic approach of binding together the readiness, the revolution in military affairs, and regional engagement with the information resources needed to accomplish the mission.

10.3 INTRODUCTION: INFORMATION CAPABILITIES FRAMEWORK

10.3.1 NEED FOR AN INFORMATION CAPABILITIES FRAMEWORK

10.3.1.1 BACKGROUND

Acquisition agencies within the Department of Defense (DoD) at every level of the organization build information systems that support their individual missions. The Army, Navy, Air Force and Marines all create a proliferation of information systems to support their functional needs. These independent efforts produce a myriad of effective solutions within a limited scope of the DoD Enterprise. Many of these systems were often in close proximity, yet isolated by differences in security measures, electronic communication, and information-sharing protocols. Functional mission commanders deployed multiple systems often with separate, dedicated transmission systems. Weapon systems on our ships each had their own sensor system and a separate communications system to send data back to the shooter. Our networks are often “stovepiped” – they are neither inter-connected nor interoperable.

At present, the DoD Infostructure is a collection of information resource solutions assembled from multiple system developers, program managers and other solution providers. Each solution within the Infostructure is replaced as new ones arise that are more capable or less expensive. To support the principles of innovation and co-evolution, a common ubiquitous underlying framework is needed to harness the changes inherent in implementing information technology to maximize capability. The true power of information comes from an integrated enterprise. The ICF provides the grid upon which solutions can be connected and contribute synergistically to the Infostructure.

10.3.1.2 PURPOSE

The purpose of the ICF is to provide a requirements grid upon which systems and efforts will overlay to portray their contribution to end-to-end capability. This is markedly different from process diagrams that lead to systems for point (stovepiped) solutions. The ICF works in conjunction with the traditional C4ISR Architecture Framework that calls for operational architectures, system architectures and technical architectures. The ICF organizes and relates efforts as well as systems. It supports the evolution of architectures over time and provides the structure needed for change management.

10.3.2 INFORMATION SUPERIORITY

The ICF provides the structural underpinning upon which to assemble the infrastructure needed to achieve Information Superiority in accordance with Joint Vision 2020 (JV2020).

Per JV2020, *information superiority* is the ability to collect, process, protect, and distribute relevant and accurate information in a timely manner while denying this capability to adversaries.

Information superiority is the ultimate force multiplier. It is the critical enabler of the transformation and adaptation needed to respond to rapidly changing situations, as well as evolving technology. In terms of national security, warfighting and warfare support, it provides:

- More effective force synchronization
- Increased speed of command
- Higher tempo of operations
- Greater lethality
- Less fratricide and collateral damage
- Increased survivability
- Decreased vulnerability
- Streamlined combat support
- Sharing of information among different security domains

Information superiority starts with the ability to collect the information needed to support operations. The importance of interoperability -- the ability of different organizations and systems to share and utilize information -- is paramount. Without a comprehensive approach to integrating U.S. Pacific Command's (USPACOM's) information processes and to achieving interoperability across organizations and systems, gaps and barriers will diminish the quality, quantity, and timeliness of information available for operations. The promise of shared awareness is in synchronized efforts. Not only is it important that situation-related information is shared, but also that there is a capability for collaborative decision-making and sharing of the commander's perspective, intent, plans, and implementing actions. These create the conditions necessary to dynamically synchronize actions in response to developing situations, and to take advantage of opportunities as they occur.

The ability to move information quickly to where it is needed and to create shared awareness provides an opportunity to develop new concepts of operation and new approaches to Command and Control (C2) that are more responsive and offer

greater flexibility. To achieve their full potential, these new concepts may require changes in organization, doctrine, material, and the like - changes that need to be co-evolved along with the development of new operational concepts and approaches to command and control. New approaches to C2 will achieve greater agility, flexibility and capability for force self-synchronization through integration of the planning and execution processes that are currently separate and sequential. Based upon a common understanding of the situation and the commander's intent, these forces will be able to respond rapidly in a coordinated fashion. Information superiority provides enhanced flexibility and agility, allowing U.S. forces to be more proactive and shape the battlefield.

The ICF provides the structure and common frame of reference to guide the continuous changes in organization, doctrine, material and associated systems required to achieve and maintain information superiority. The ICF will foster harmonious change and avoid the inefficiencies that accompany the lack of structure associated with the cyber environment.

10.3.3 THE INFOSTRUCTURE

Information superiority requires a critical mass of protected information, information processing capabilities, trained personnel, and assured connectivity, so warfighters and warfare supporters can take advantage of the power of information and the possibilities of networking. This is referred to in the Secretary of Defense's Annual Report to the President and Congress as the *Infostructure*. For the ICF, the Infostructure is the single term that refers to the comprehensive, end-to-end collection of information resources across the DoD to maximize operational effectiveness and enable achievement of information superiority for the warfighter.

At the most abstract level, the ICF uses a generic framework model to describe the Infostructure as illustrated in Figure 4. As shown, there are three major areas of the Infostructure: the planning, policy and architecture components, the system and infrastructure components and the process and support components. The ICF is the framework used to describe the present, planned and proposed Infostructure components.

Section 4 will develop the ICF as shown in Figure 4.

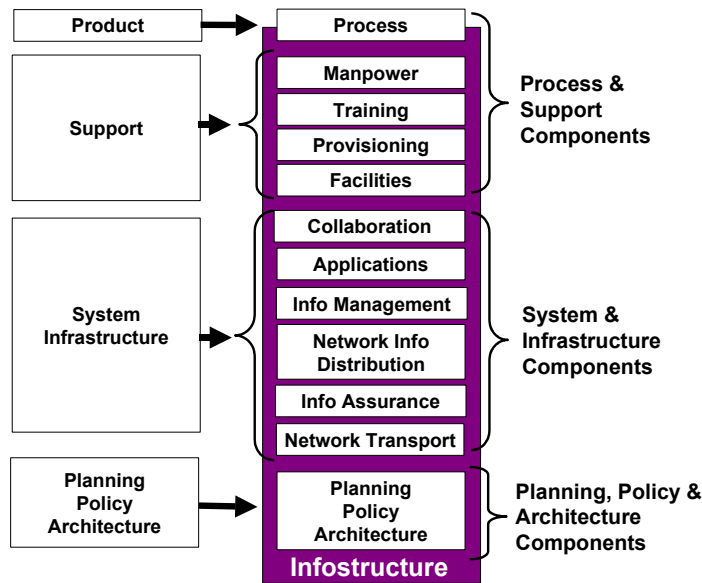


Figure 10-4. Illustration of the Infostructure

The creation of the Infostructure is not a one-time milestone, but rather a continuing process to identify the best that technology has to offer and adapt it to the needs of USPACOM. Central to this effort is a continuing emphasis on security, advanced technology, integration of multiple technologies into a coherent capability, and interoperability.

10.3.4 CHIEF INFORMATION OFFICER (CIO) SYSTEM IMPLEMENTATION PRECEPTS

The quality of USPACOM's Infostructure will be the pacing item on the journey to the future. The ability to conceive of, experiment with, and implement new ways of doing business to leverage the power of information age concepts and technologies depends upon what information can be collected, how it can be processed, and the extent to which it can be distributed. In turn, the ability to bring this capability to war will depend upon how well it can be relied upon in terms of security and dependability. We envision an Infostructure that is seamless with built-in security; one that can support the need for increased combined, joint, and coalition interoperability, and one that leverages commercial technology and accommodates evolution.

Seamless and Coherent. To facilitate the end-to-end flow of information necessary to support network-centric operations, information processes must be transparent to users. We must lead the effort to transition USPACOM systems from isolated, stovepiped environments to a seamless and coherent Infostructure. This transition requires the establishment of a USPACOM-wide mechanism for gaining visibility into the many separate planning, budgeting, acquisition, operations, and maintenance activities that contribute to USPACOM's information systems and processes. DoD's Global Information Grid (GIG) is designed to achieve this by creating a DoD-wide network management solution. This solution is comprised of enterprise network policies, strategies, architectures, focused investments, and network management control centers that bring order out of the currently fragmented Service-centric DoD information infrastructure.

Built-In Security. While the information age created enormous opportunities, it also created significant vulnerabilities for those who depend on an uninterrupted flow of quality information to support operations. Protecting USPACOM information and information assets is not a luxury. It is a basic necessity. Protection must be engineered-in from the outset, not added on as an afterthought. Security must be co-evolved with approaches to interoperability because new/revised links among systems increase vulnerabilities. While DoD's continuing migration from analog to digital systems will facilitate efforts, there will always be legacy systems and systems used by coalition partners, that lack adequate security. USPACOM is exploring approaches to deal with these exceptions. However, these approaches will, in all likelihood, entail limiting the functionality and utility of these nonconforming systems.

Joint and Coalition from the Start. Despite provisions in our acquisition regulations that direct new systems to be built for operation in a joint environment, the practice is to start single-service, then add joint and combined links later in the process. The unfortunate result is a loss of combat power. Future operations will be joint or multi-service, include reserve components, and will most likely involve partnerships with other countries to form a coalition. Their effectiveness will depend upon the ability of USPACOM to share information and collaborate internally and externally. Therefore, interoperability must be considered a key element in all DoD operational and systems architectures. Experience shows that after-the-fact interoperability fixes are costly, do not satisfy mission requirements, and create security problems. As with security, success is achieved by incorporating interoperability from the start.

Leverages Commercial Technology. DoD benefits from the enormity of the commercial marketplace for information technology which drives down the costs of off-the-shelf capabilities, and fuels an unprecedented rate of improvement in cost and performance. USPACOM can reap the benefits of private sector investments, thereby channeling R&D investment into militarily

significant areas the commercial sector is not addressing. However, we must balance use of commercial technology with the requirement to ensure security is built in from the start.

Accommodates Evolution. Change is the constant of the information age. USPACOM's Infostructure must be designed to accommodate rapid change as both requirements and technologies evolve. A comprehensive strategy that consists of appropriate architectures, standards, design principles, configuration management, and regression testing will be incorporated into USPACOM's Infostructure processes.

10.4 AN ENDURING FRAMEWORK FOR A DYNAMIC ENVIRONMENT

10.4.1 CHARACTERIZING DEPENDENCIES BETWEEN CAPABILITIES

Capabilities are highly inter-related, especially those provided by information technology. An enduring framework requires a standard way of depicting capability relationships. This will allow for system assignments to be reused in multiple mission areas. This construct allows for easy identification of common requirements/capabilities that can be optimized in order to avoid stove-piped system implementation with a performance impact on the Infostructure that is less than optimal.

These capabilities can be divided into three tiers: foundation capabilities, functional capabilities, and mission capabilities. The purpose of these tiers is to foster a modular approach to achieving end-to-end capability by assembling specific capability components. The three tiers also convey how "sharable" a particular capability component is. *Foundation capabilities* are the most sharable, and support a wide array of functional capabilities. An example of a foundation capability is network transmission for communications. Network transmission for communications, as a capability, is the foundation component of almost end-to-end capability under the Network Centric Warfare concept. *Functional capability* is more specific to a particular mission or operation. Functional capability is also sharable across multiple mission areas, but often relies upon the foundation capabilities. *Mission capability* is the combination of the foundation and functional capabilities needed to accomplish the mission. The key point is that you have to invest in the foundation layers first, before you reap the benefits of the upper layers. Following this process is crucial to preventing the development of stovepipe, standalone systems. Figure 5 illustrates.

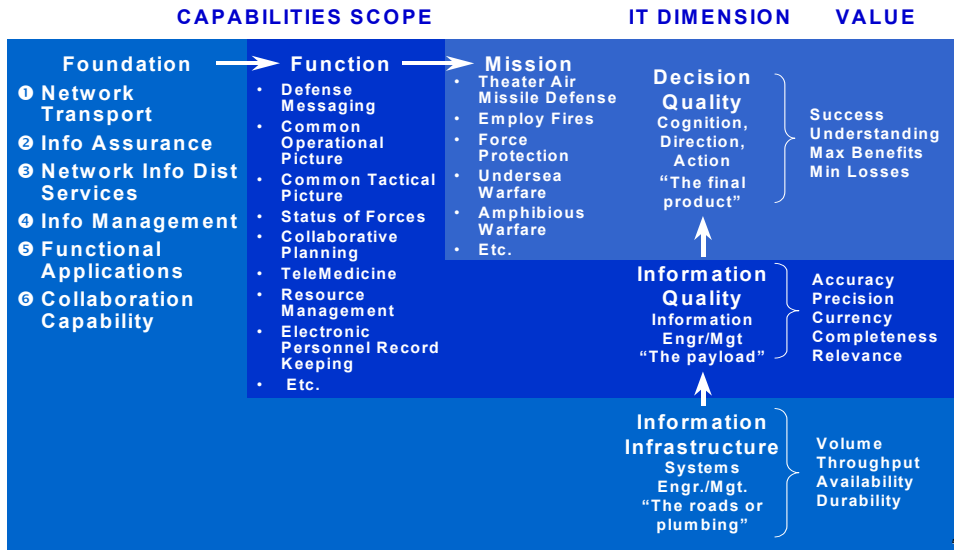


Figure 10-5. Using Capabilities Scope to Manage Interdependencies

10.4.2 RELATIONSHIP OF OTHER PARADIGMS TO THE ICF

The system and infrastructure group within the ICF is not the same as the standard seven-layer Open Systems Interconnect (OSI) model. As shown in Figure 6, the entire OSI model is contained within the bottom two layers of the information and systems group of the ICF.

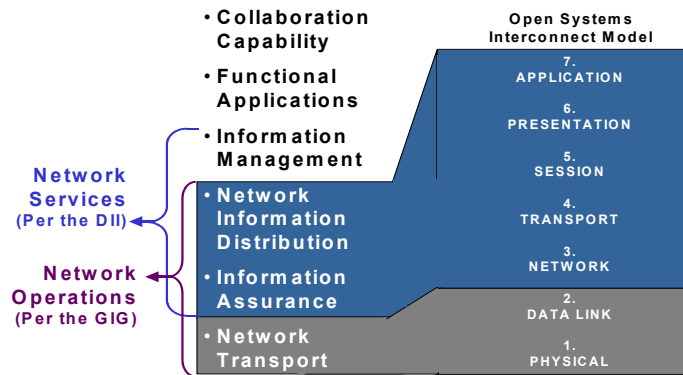


Figure 10-6. Comparison of the ICF to the Seven Layer OSI Model

As a foundation capability, the Infostructure provides the underpinning for all information superiority related operations. Information superiority, in turn, provides the underpinning for all other warfare capability within the paradigm of network centric warfare and JV2020. It is, therefore, extremely important to treat the Infostructure as critical warfighting capability that must be protected and resourced as well as, or better than, the actual platforms that deliver ordnance. This is especially true when considering Effects-Based Operations (EBO) where kinetic destruction is not necessarily the prime objective of an operational mission.

Proper treatment of this critical operational capability that cuts across all U.S. and allied military services would dictate that it be given common nomenclature. However, the defense community has yet to come to terms with the Infostructure as being a critical military capability. It is often confused with the support infrastructure associated with providing electricity. Consider Figure 7, which provides the various names provided to the Infostructure by several elements of the DoD. It would be helpful, though not essential, if we could use the same nomenclature for the Infostructure. This would help communicate to program managers and system developers that they are not implementing entire closed systems, but components of the overall Infostructure that must be refreshed over time. This would also help to develop methods and converge systems into what would appear to the operators as a single integrated system with tight coherency between applications. This would achieve the CIO's principle of a "seamless and coherent" infrastructure because the underlying complexity of the Infostructure would be transparent to the user.

In summary, to support maximum information integration, sharing and protection within compressed time frames, it is best that the Infostructure behave as a single, tightly integrated system with minimal seams. However, the Infrastructure must also satisfy the need to refresh systems to exploit new technology and innovative resources, per the principles discussed in Section 10.3.2 and Infostructure. The complexity associated with this challenge is daunting unless the Infostructure is divided into categories that will channel system implementations into tightly integrated capabilities.

Source	Abr.	Term
SECDEF*		"Infostructure"
OSD	GIG	Global Information Grid
Intel. Community	DoDIIS	DoD Intel. Info. System
DISA	DII	Defense Info. Infrastructure
JV-2010	ITP	Info. Transport & Processing
Joint Staff (P-JMAs)	CCE	Comms & Computer Env.
US Navy	CISN	Comms & Info System Networks

* - Chapter 8 - Annual report to the President and Congress

Figure 10-7. Terms Used in DoD to Describe the 'Infostructure'

10.5 USING THE INFORMATION CAPABILITIES FRAMEWORK

As stated in Section 3, the Information Capabilities Framework (ICF) provides the requirements grid onto which systems and efforts must overlay to portray their contribution to end-to-end capability. It shows the interdependencies and how each system component contributes to the Infostructure and to information superiority. This chapter provides guidance on how to use the ICF to maximize effective and efficient operations.

10.5.1 INFORMATION INFRASTRUCTURE STATUS REPORTING

Without an organizing framework, the Infostructure is a complex and confusing array of systems including networks, server suites, databases and the like. The ICF allows mapping of the systems into capability areas to provide a common frame of reference. This is necessary to perform domain assessments across the enterprise involving multiple organizations and domains, and over time, for trend analysis. Figure 3 provides an example of how the ICF is used in the USPACOM Theater Command, Control, Communication and Computer Systems (C4) Coordination Center (TCCC) to display the Infostructure status across the theater. Figure 8 displays the associated Infostructure status trend over time.

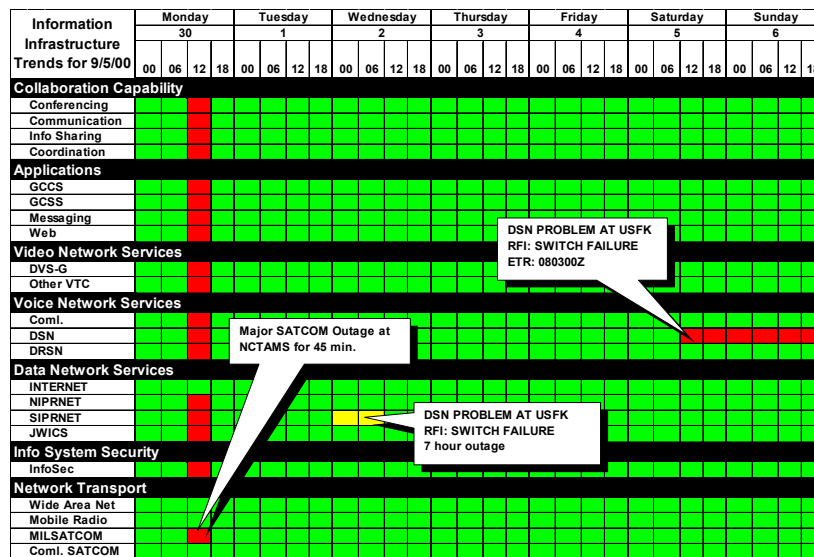


Figure 10-8. Using the ICF to Depict System Status Trends

10.5.2 SYSTEM IMPLEMENTATION PLANNING

The ICF can be used to organize various aspects of system implementation from planning through installation and training. This outline can be used in Operational Plan Annex K (Communication Support) to track plan requirements and the status of efforts to meet the Infostructure capability requirements. Figure 9 illustrates.

Information Infrastructure	Concept	Policy	Governance	Standards	Procedures	Guidance	Training
Collaboration Capability							
Conferecing	Yellow	Red	Red	Yellow	Red	Red	Red
Communication	Yellow	Red	Red	Yellow	Red	Red	Red
Info Sharing	Yellow	Red	Red	Yellow	Red	Red	Red
Coordination	Yellow	Red	Red	Yellow	Red	Red	Red
Applications							
Web Apps	Green	Green	Green	Green	Green	Green	Green
Messaging	Green	Green	Green	Green	Green	Green	Green
GCCS	Green	Green	Green	Green	Green	Green	Green
GCSS	Green	Green	Green	Green	Green	Green	Green
Video Network Services							
DVS	Green	Green	Green	Green	Green	Green	Green
Other VTC	Green	Green	Green	Green	Green	Green	Green
Voice Network Services							
ComL Voice	Green	Green	Green	Green	Green	Green	Green
Radio Voice	Green	Green	Green	Green	Green	Green	Green
DSN	Green	Green	Green	Green	Green	Green	Green
DRSN	Green	Green	Green	Green	Green	Green	Green
Data Network Services							
INTERNET	Green	Green	Green	Green	Green	Green	Green
NIPRNET	Green	Green	Green	Green	Green	Green	Green
SIPRNET	Green	Green	Green	Green	Green	Green	Green
JWICS	Green	Green	Green	Green	Green	Green	Green
Info System Security							
InfoSec	Green	Green	Green	Green	Green	Green	Green
Network Transport							
Mobile Radio	Green	Green	Green	Green	Green	Green	Green
MILSATCOM	Green	Green	Green	Green	Green	Green	Green
ComL SATCOM	Green	Green	Green	Green	Green	Green	Green
Wide Area Net	Green	Green	Green	Green	Green	Green	Green

Concept of operations is proposed but not approved for Coordination Tools for Collaboration.

System implementation preparation is complete for all requirements shown in green.

Figure 10-9. Using the ICF to Support System Implementation

On a macro scale, the Doctrine, Organization, Training, Material, Logistics, Personnel, Administration, and Facility (DOTMLPAF) can be compared across the ICF to determine, illustrate, and track system implementation support requirements. This is shown in Figure 10.

Information Infrastructure	D	O	T	M	L	P	F
	Doctrine	Organization	Training	Material	Logistics	Personnel	Facility
Collaboration Capability							
Associated Solutions							
Applications							
Associated Solutions							
Information Management							
Associated Solutions							
Network Info Dist. Services							
Associated Solutions							
Information Assurance							
Associated Solutions							
Network Transport							
Associated Solutions							

Each of these cells would contain a link to the associated reference or to the organization providing the associated DOTMLPF support.

Figure 10-10. Using the ICF to Support DOTMLPF Planning

10.5.3 INVESTMENT MANAGEMENT, COST CONTROL AND ACQUISITION COORDINATION

The ICF can be used to map programs and solutions versus their role in the Infostructure and the associated costs and appropriation as illustrated in Figure 11. The framework can also be used to coordinate implementation of acquisition programs and prototypes, by breaking the associated systems into system components to map into the associated capability categories as shown in Figure 12.

Information Infrastructure	PROGRAMS							TOTALS
	Organizational Unit	Organizational Unit	Organizational Unit	Organizational Unit	Organizational Unit	Organizational Unit	Organizational Unit	
Collaboration Capability								
Associated Programs	\$\$	\$\$	\$\$	\$\$	\$\$	\$\$	\$\$	\$\$
Applications								
Associated Programs	\$\$	\$\$	\$\$	\$\$	\$\$	\$\$	\$\$	\$\$
Information Management								
Associated Programs	\$\$	\$\$	Includes appropriations, program element, line items and the like.				\$\$	\$\$
Network Info Dist. Services								
Associated Programs	\$\$	\$\$	\$\$	\$\$	\$\$	\$\$	\$\$	\$\$
Information Assurance								
Associated Programs	\$\$	\$\$	\$\$	\$\$	\$\$	\$\$	\$\$	\$\$
Network Transport								
Associated Programs	\$\$	\$\$	\$\$	\$\$	\$\$	\$\$	\$\$	\$\$
TOTALS								
	\$\$	\$\$	\$\$	\$\$	\$\$	\$\$	\$\$	\$\$

Figure 10-11. Using the ICF to Support Investment Management

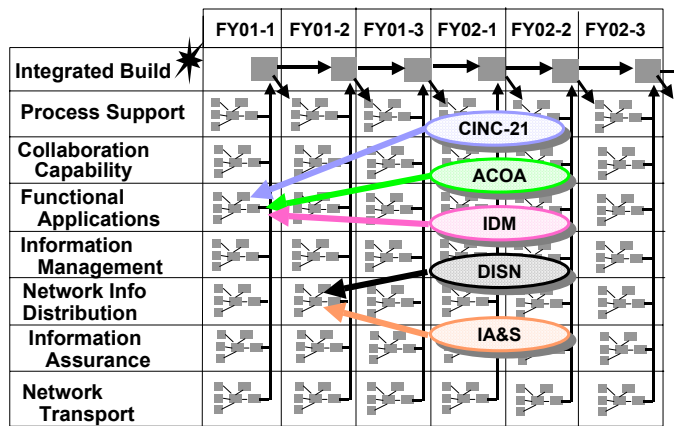


Figure 10-12. Using the ICF to Perform System Integration Management

10.5.4 RELATING THE GLOBAL INFORMATION GRID (GIG) CAPSTONE REQUIREMENTS TO THE ICF

The GIG is the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers and support personnel. It is the DoD's official enterprise network. The GIG Capstone Requirements Document provides requirements specifications for systems to be integrated into the GIG. The ICF is USPACOM's strategy to integrate information capability solutions onto the GIG. Figure 13 shows a matrix of GIG Functions versus GIG Categories and how the ICF categories relate. GIG capstone requirements are organized per the matrix shown in Figure 13. Figure 14 shows the ICF and how the GIG categories and functions relate. A separate document will show the specific relationship of each GIG capstone requirement to the ICF to map information systems and capabilities into the Infrastructure in accordance with GIG guidelines.

		GIG CATEGORIES			
		COMPUTING	COMM	PRESENTATION	NET OPS
GIG FUNCTIONS	Cells contain USPACOM ICF System and Infrastructure Categories				
	PROCESS	INFORMATION MANAGEMENT and FUNCTIONAL APPLICATIONS and COLLABORATION CAPABILITY			
	STORE	INFORMATION MANAGEMENT and FUNCTIONAL APPLICATIONS and COLLABORATION CAPABILITY			
	TRANSPORT		NETWORK TRANSPORT		
	HUMAN GIG INTERFACE			INFORMATION MANAGEMENT and FUNCTIONAL APPLICATIONS and COLLABORATION CAPABILITY	
	NETWORK MANAGEMENT				NETWORK INFORMATION DISTRIBUTION and NETWORK TRANSPORT
	INFORMATION DISSEMINATION MANAGEMENT				NETWORK INFORMATION DISTRIBUTION and INFORMATION MANAGEMENT
INFORMATION ASSURANCE				NETWORK INFORMATION DISTRIBUTION and INFORMATION ASSURANCE	

Figure 10-13. ICF Relationship to the GIG CRD

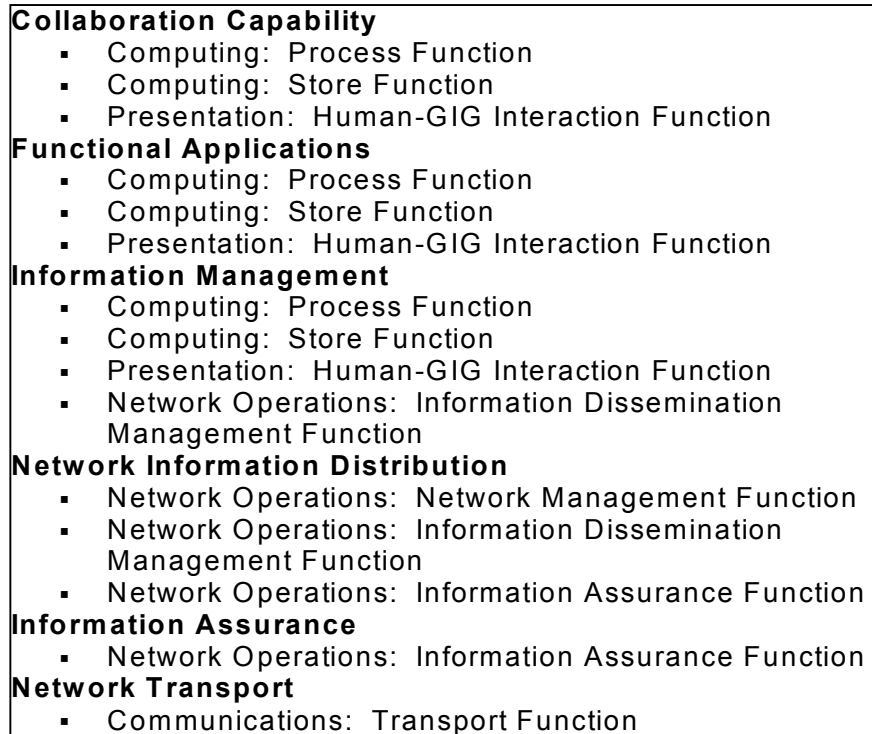


Figure 10-14. GIG CRD Categories Captured Within the USPACOM ICF

10.5.5 RELATING JOINT MISSION AREAS, ESSENTIAL TASK LISTS, FUNCTIONAL AREAS AND PROCESSES

To illustrate how the ICF relates to doctrine such as Joint Mission Essential Tasks and Joint Mission Areas, mission capability is shown as the focus. Figure 7-26 shows these relationships and illustrates that mission capability is the intersection of tasks, processes, and functions.

To drill down, start with the process framework discussed in Section 7.4.5 and shown in Figure 7-38. All processes use the same "knowledge sphere" so they can share information, collaboration, and applications.

Further drilling down into the "knowledge sphere," Figure 15 shows the organization of functional applications and information that use ICF categories. Figure 16 shows the same diagram in a linear format which is preferred by the

Intelligence Community's (IC's) System Integration Management (SIM) process. Also, according to the SIM process, each application and how it relates to a Joint headquarters organization is shown in Figure 17.

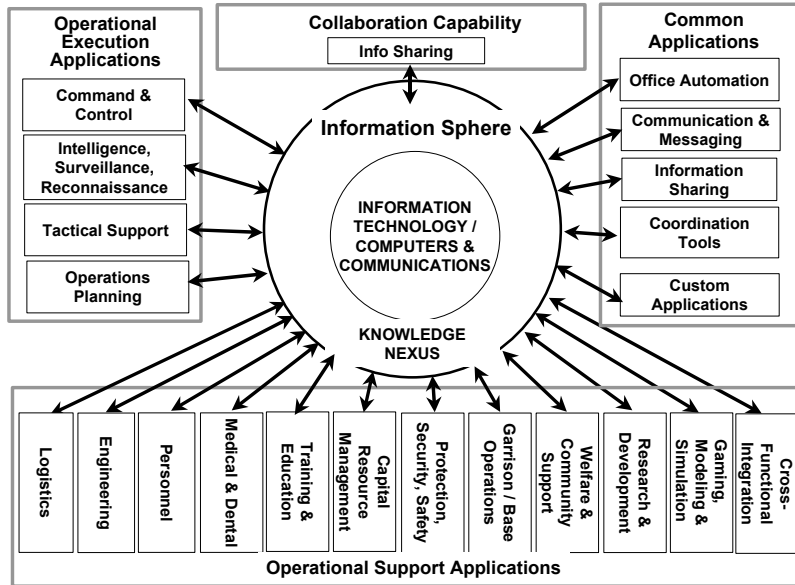


Figure 10-15. Illustration of the Application Layer Using the Information Layer as the Hub

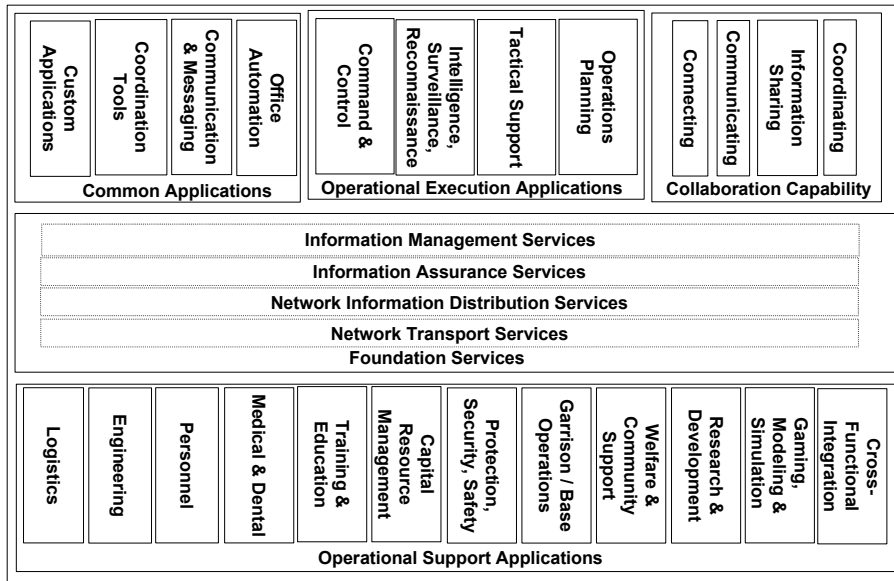


Figure 10-16. Infostructure in System Integration Management Format

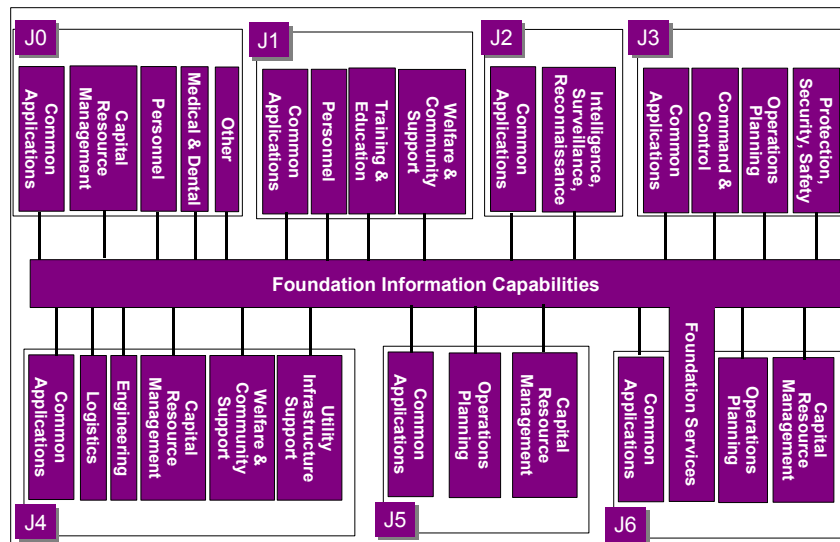


Figure 10-17. Infostructure in System Integration Management (SIM) Format for a Joint HQ Staff

10.5.6 USING THE IFC TO DEPICT SYSTEM ARCHITECTURES

The ICF can be used to provide a method to develop consistent depictions of system architectures. The following definitions and schemas are presented to translate the ICF into architectures that can be used to relate to each other and to depict the status of end-to-end capability:

System. The information and data processing resources, associated peripheral devices, supported applications, and the communications network infrastructure that interconnects the end users and components of the system. Systems include hosts, operating systems, peripherals and system applications, databases, and files. A system also includes all hardware and software components, facilities, personnel, and procedures that are necessary to support applications.

Network. The set of switching and transmission subsystem communication components to support information transfer. The network includes all hardware and software communication components residing in switching, routing, and transmission subsystem components, as well as communication-related hardware and software and those components that reside in hosts (e.g., communication protocols). The network also includes the organization and configuration of embedded hardware and software to support orderly and logical information distribution.

Application. A collection of system components that supports a particular task or function. It includes end-to-end, multi-media communications as well as information management and decision support capability. Distributed computing applications are normally built using a three-tiered architecture that consists of the application server, data server, and presentation clients which may be physically on a single device or on multiple devices connected by a network. Communication applications normally involve a minimum of two communication devices connected by the network.

Appliance. Any device by which an end user receives, processes, or transmits information on the selected media. Information appliances include computers, telephones, televisions, video teleconferencing equipment and the like. It is also the hardware component that is part of an information appliance suite such as a mouse, keyboard, or video screen. In the three-tiered application architecture, these devices are referred to as “presentation clients”.

Information. The assembly and presentation of data in a form that is understandable and valuable for conveying knowledge and making decisions. It is the “payload” of the information infrastructure.

The network forms the foundation for the system, applications and appliances. Appliances are the user's interface which connect to the network so that data and applications can be accessed. Applications are the software programs, information tools, and databases the user operates to perform tasks. Applications transcend the network and the appliances. They involve multiple distributed computers and databases including the data server, application server and presentation client software. Application management includes coordination of the network managers and appliance managers so that the program software can access the data and processors needed.

Figure 18 and Figure 19 respectively provide illustrations of the operator's perspective and the system manager's perspective of these system infrastructure categories.

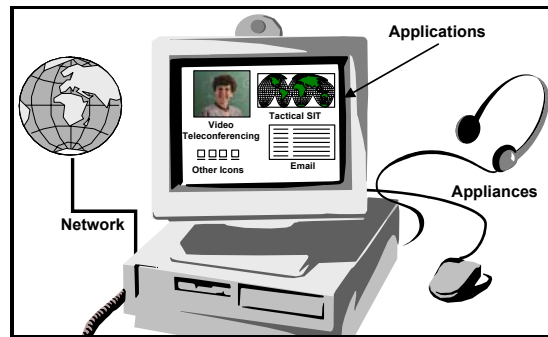


Figure 10-18. User's View of the Infostructure

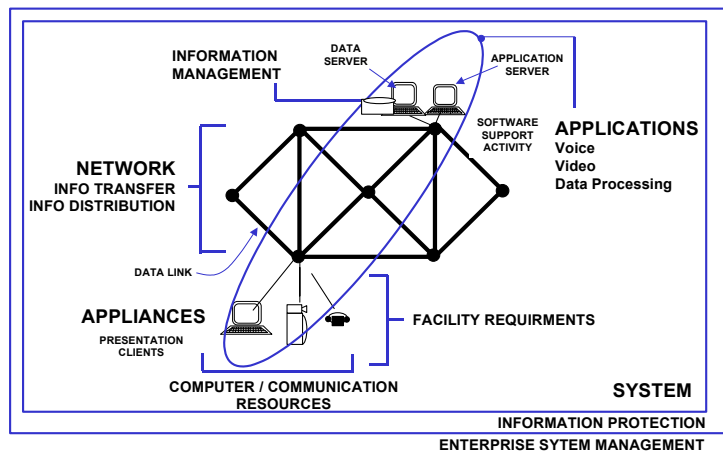


Figure 10-19. System Manager's Perspective of the Information Infrastructure

The operator interfaces with the computer, video equipment, headset or telephone and cares about running applications, receiving and transmitting information independent of the physical location of the information.

The system manager cares about appliances, network nodes, links and associated equipment. He also cares about interoperability of the software across the network, with the appliances, various databases and software management facilities that support the end user's application.

Figure 20 shows the system manager's depiction using four layers of the ICF reflecting network transport and information distribution, information assurance, information services and application services, respectively. Figure 21 shows three cases of application implementations. The top layer shows locally managed servers providing services to remote clients. The middle layer shows local clients accessing remote servers. The bottom layer shows local clients accessing local servers. Figure 22 illustrates the collection of systems within this architectural framework for USCINCPAC's HQ-21 new headquarters project.

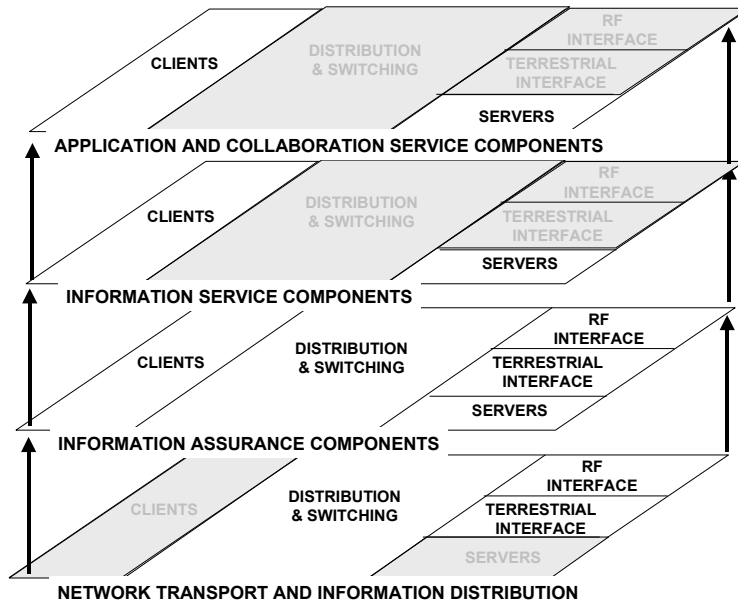


Figure 10-20. Using the ICF to Support Creation of System Architectures

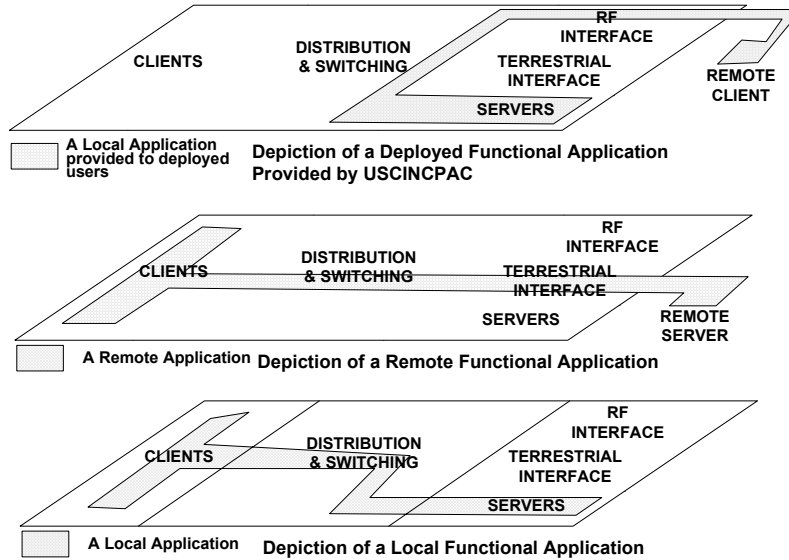


Figure 10-21. Showing System Footprints on the ICF Architecture

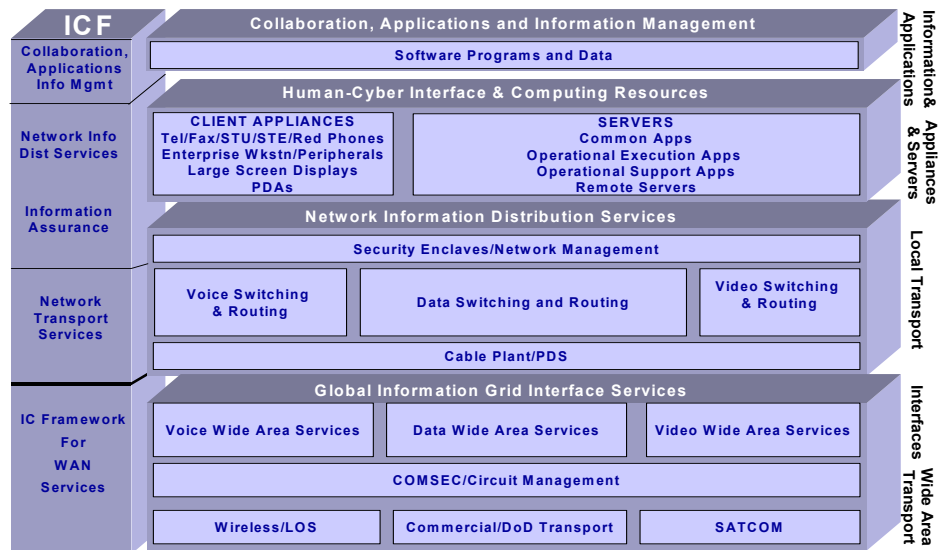


Figure 10-22. ICF Support of the USCINCPAC New Headquarters

10.6 CONCLUSION

The ICF is a critical component of information superiority in that it defines how all information resources relate to each other to provide end-to-end information integration, sharing and protection capability. The overall system-of-systems including both hardware and software is referred to as the Infostructure.

The ICF is only useful if it is able to achieve long-term stability in the face of technology that is changing at Internet speed. It also must relate information systems and efforts to warfighting capability. Three major components of the ICF were defined: (1) Planning, Policy and Architecture (2) System and Infrastructure, and (3) Process and Support. Each of these components was discussed in their own follow-on chapter.

Section 7.1 described the planning, policy and architecture components that depend heavily on the C4ISR Architecture Framework and DoD Information Assurance requirements.

Section 7.2 described each of the six layers of the system and infrastructure components of the Infostructure. These layers are:

- Network Transport
- Information Assurance
- Network Information Distribution
- Information Management
- Functional Applications
- Collaboration Capability

The first three layers are primarily hardware and the last three layers are primarily software.

Section 7.3 described the future system and infrastructure layers. These future layers are required to foster development of a single ubiquitous network. As much as it was hoped to have today's systems and efforts characterized by the future Infostructure, this was found to be too far from today's reality. However, the organization described in Section 7.3 will help foster the development of the objective architecture, once today's systems and efforts are captured in terms of the ICF described in Section 7.2.

Section 7.4 described how the ICF characterizes Infostructure support components in terms of facilities, provisioning, manpower and training. It categorizes efforts to connect the system infrastructure with operations and business processes.

Section 10.5 described how the ICF can be used to organize IT and IM efforts to maximize operational effectiveness, acquisition and implementation efficiency.

Section 10.6 is the conclusion and summarizes the ICF document.

Ultimately, the ICF will foster the development and implementation of information resources so the warfighter, and those in support, will be fully empowered. This empowerment will result in the capability to access the information they need, in a form they can use to develop knowledge, form teams independent of time and space, and make good decisions in compressed time frames, thereby maximizing overall mission effectiveness. It also enables the planners and supporters to develop missions, and to determine the right missions. It enables top DoD leadership to effectively shift between transactional and transformational management methods as needed, to guide the DoD Enterprise to meet the needs of the nation.

APPENDIX A- ACRONYMS

Acronym	Expansion
ACOA	Adaptive Courses of Action ACTD
ACTD	Advance Concept Technology Demonstration
ALCOM	Alaskan Command
APAN	Asia Pacific Area Network
ASD(C3I)	Assistant Secretary of Defense for C3I
ARPAC	U.S. Army, Pacific
C2	Command and Control
C2S2	Command and Control Support System
C3I	Command, Control, Communications and Intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIA	Central Intelligence Agency
CIPO	CINC Interoperability Program Office
CINC	Commander-in-Chief
CINC-21	Commander-in-Chief for the 21st Century ACTD
CIO	Chief Information Officer
CJCS	Chairman, Joint Chiefs of Staff
CM	Configuration Management
COO	Chief Operating Officer
CONOPS	Concept of Operations
CONT	Abbreviation for Contractor

COP	Common Operational Picture
COS	Chief of Staff
COWAN	Combined Operations Wide Area Network
CRD	Capstone Requirements Document
CTL	Combined Theater Logistics
CTO	Chief Technical Officer
CUE	Common User Environment
DAA	Designated Approval Authority
DAB	Defense Acquisition Board
DCINC	Deputy Commander-in-Chief
DCOS	Deputy Chief of Staff
DITSCAP	Defense Information Technology Security Certification and Accreditation Program
ELB	Extending the Littoral Battlespace ACTD
FOIA	Freedom of Information Act
GAO	General Accounting Office
GIG	Global Information Grid
GPRA	Government Performance & Results Act
G&PM	Guidance & Policy Memorandum
HQ	Headquarters
HQ-21	21st Century Headquarters Project
I4C	Integrity, Information, Integration & Innovation for the Customer
IA	Information Assurance
IC	Intelligence Community
IDM	Information Dissemination Management
IM	Information Management

IM/IT	Information Management / Information Technology
IMSP	Information Management Strategic Plan
INFOSEC	Information Security / Information Systems Security
IO	Information Operations
IPT	Integrated Product Team
IRM	Information Resource Management
IRMS	Information Resource Management System
ISPCS	Information System Project Coordination System
ISSA	Information Systems Support Activity
ISSO	Information Systems Security Officer
ISSM	Information Systems Security Manager
IT	Information Technology
ITMRA	Information Technology Management Reform Act
ITSG	Information Technology Standards Guidance
JC	Joint Community
JCAPS	Joint C4ISR Architecture and Planning System
JFCOM	Joint Forces Command
JIATF	Joint Inter-Agency Task Force
JICPAC	Joint Intelligence Center, Pacific
JMF	Joint Mission Force
JMO-T	Joint Medical Operations - Telemedicine ACTD
JROC	Joint Requirements Oversight Council
JTF	Joint Task Force
JTF FA	Joint Task Force, Full Accounting
KPP	Key Performance Parameters

MUE	Mobile User Environment
NMCI	Navy - Marine Corps Intranet
NSA	National Security Agency
NSS	National Security Systems
ORD	Operational Requirements Document
PACAF	Pacific Air Forces
PACFLT	Pacific Fleet
PACOM	United States Pacific Command
PBAC	PACOM Budget Action Council
PCITS	Process and Capabilities Information Tracking System
PRA	Paperwork Reduction Act
R&D	Research & Development
RDT&E	Research Development, Test & Evaluation
RBA	Revolution in Business Affairs
RMA	Revolution in Military Affairs
SA	System Administrator
SECDEF	Secretary of Defense
SES	Senior Executive Service
SIMDB	System Integration Management Database
SOCPAC	Special Operations Command, Pacific
TIG	Theater Information Grid
TUE	Team User Environment
U.S.	United States
USA	United States Army
USAF	United States Air Force

USC	United States Code
USF	United States Forces (used with Japan, Korea)
USCINCPAC	United States Commander-in-Chief, Pacific Command
USMC	United States Marine Corps
USN	United States Navy
USPACOM	United States Pacific Command
VIC	Virtual Information Center

APPENDIX B- DEFINITIONS

Term	Definition
Application Services	Availability of servers to process data to provide results for numerous uses including decision support, modeling, simulation, analysis and the like. Used in conjunction with Information Services.
Architecture	An organized framework consisting of principles, rules, conventions, and standards that serve to guide development and construction activities such that all components of the intended structure will work together to satisfy the ultimate objective of the structure. (Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2dEdition, Electronic Version)
Business Process Improvement	A systematic approach to help an organization make significant advances in the way its business processes operate. It defines an organization's strategic goals and objectives and aligns its processes to better meet customer requirements. (Federal Aviation Administration BPI Home Page www.faa.gov/ait/bpi/bpihome.htm (18NOV00))
Capstone Requirements Document	Document that captures the overarching requirements for a mission area that forms a family-of-systems (FoS) or System-of-Systems (SoS). They are intended to guide the DoD components in developing mission needs and operational requirements documents for future and legacy systems. (CJCSI 3170.01A, 10AUG99)
Chief Executive Officer	In an organization with a board of directors, the CEO is the singular organizational position that is primarily responsible to carry out the strategic plans and policies as established by the board of directors. Without a board of directors, the CEO is the singular organizational position that sets the direction and oversees the operations of an organization. (McNamara, Carter, MBA, PhD, Management Assistance Program for Non-Profit Organizations (www.mapnp.org) (18NOV00))
Chief Information Officer	The executive who is accountable for directing the information and data integrity of the enterprise and its groups and for all Information Service functions of the enterprise including data centers, technical service centers, production scheduling functions, help desks, communication networks (voice, video and data), computer program development, and computer system operation. (CIO Magazine, www.cio.com (19NOV00))
Chief Operating Officer	Executive responsible for the day-to-day operations of an enterprise.
Chief Technical Officer	Executive who directs an organization in matters pertaining to technology. (www.computeruser.com (19NOV00))
CIO Advisory Groups	Various councils, committees and forums allowing formal participation by all members of the U.S. Pacific Command to identify requirements, assign priorities and provide guidance to the CIO and his staff and allow the CIO to issue policy, directives and guidance.

Coherent	Marked by an orderly, logical, and aesthetically consistent relation of parts. (American Heritage Dictionary of the English Language, 1996)
Collaboration	To work together, especially in a joint intellectual effort. (American Heritage Dictionary of the English Language, 1996)
Command and Control	The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. (JP 1-02, 23MAR94 amended 1SEP00)
Common User Environment	Workstations, peripherals, operating system, software, configurations and connections that provide a standardized set of communication and computing resources to connect to Information Services and Application Services.
Context	The part of a text or statement that surrounds a particular word or passage and determines its meaning. The circumstances in which an event occurs; a setting. (American Heritage Dictionary of the English Language, 1996)
Data	Symbols representing instances, or occurrences, of specific meanings in the real world. (Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2d Edition, Electronic Version)
Designated Approval Authority	Command official who is directly responsible for information system security policy that considers risk, what is at stake, the operational situation versus the operational benefit of information sharing. (Derived from DOD CIO GIG G&PM 6-8510)
Decision Support Workspace	An assembly of "views" which provides information and knowledge needed to support a decision or set of decisions. Decision support workspaces are useful for shared awareness on large screen displays or commonly viewed monitors.
DITSCAP Process	Process which demonstrates that a system or system configuration can be operated with acceptable security risk within the operating environment and conditions specified.
Engagement	The act of involving an organization or entity.
Enterprise	When used generically, an enterprise is defined as the aggregate of all functional elements participating in a business process improvement action, regardless of the organizational structure housing those functional elements. (Note the difference in this definition and that of ENTERPRISE LEVEL.) (Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2d Edition, Electronic Version)
Enterprise Level	Provides the geographic, technological, and managerial platform upon which all information systems development activity is based; it is the foundation that must support all that is built above it in the higher levels. In general, in this document it is synonymous with the entire Department of Defense. (Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2d Edition, Electronic Version)

Evolution	A gradual process in which something changes into a different and usually more complex or better form. (American Heritage Dictionary of the English Language, 1996)
Global Information Grid	A globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. (DoD CIO GIG Memo, 22SEP99)
Guidance & Policy Memorandum	Memorandum used for rapid promulgation of CIO policy and guidance to allow expedient communication of important issues before they can be integrated into the standing set of formal information such as instructions or directives.
Information	Any communication or reception of facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium, including computerized databases, paper, microfilms, or magnetic tape used to increase understanding. (Derived from DoDD 8000.1 of 27 October 1992)
Information Assurance	Information operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DoD S-3600.1)
Information Capability	The ability to access and process information needed to accomplish tasks, reduce uncertainty, increase knowledge, make sound decisions and take action with confidence, even in compressed time demands, anytime, anywhere.
Information Consumer	One that takes in information for direct use or ownership.
Information Management	The planning, budgeting, collecting, collating, correlating, manipulating, fusing, storing, archiving, retrieving, controlling, disseminating, protecting, and destroying of information throughout its life cycle.
Information Operations	Information operations (IO) involve actions taken to affect adversary information and information systems while defending one's own information and information systems. They apply across all phases of an operation, the range of military operations, and at every level of war.
Information Producer	Those organizations or individuals who are willing to be accountable for a set of business data, collections or processes by insuring their accuracy and quality for the well being of the larger organization.
Information Resources	Information and related resources such as personnel, equipment, funds and information technology. (44 USC Sec. 3502 (PRA (95)))
Information Resource Management	Process of managing information resources to accomplish agency missions and to improve agency performance including through the reduction of information collection burdens on the public. (44 USC Sec. 3502 (PRA (95)))
Information Security	The protection of information against unauthorized disclosure, transfer,

	modification, or destruction, whether accidental or intentional.
Information Services	Availability of servers to access data and information in response to research queries, reports or to feed Application Services or to process on a client computer for further rendering.
Information Set	A logical grouping of information elements.
Information Superiority	The ability to collect, process, protect, and distribute relevant and accurate information in a timely manner while denying this capability to adversaries. (JV2020)
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (44 USC Sec. 3502 (PRA (95)))
Information System Security Manager	Organization's focal point for policy and guidance on IA matters. Provides policy and program guidance to subordinate activities. (DOD CIO GIG G&PM 6-8510)
Information System Security Officer	Officer assigned to a particular system to ensure cognizant systems are operated, used, maintained and disposed of IAW accreditation. (DOD CIO GIG G&PM 6-8510)
Information Technology	Any equipment or interconnected system or sub-system of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. This includes equipment used by a Component directly or used by a contractor under a contract with the Component which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term also includes computers, ancillary equipment, software, firmware and similar procedures services (including support services), and related resources. Notwithstanding the above, the term does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.
Information Technology Services	Provisioning for use of Information Technology.
Information Worker	Any user, consumer, producer, analyst, staff member or decision-maker that uses information or information systems in the conduction of operations or business. (Just about everyone.)
Information Infrastructure	The underlying base or foundation of communication networks, computers, software, databases, applications, application system interfaces, data, security services and other services that meet the information processing and transport needs of users across the range of operations. (Derived from DII Master Plan Ver 7.0 13MAR98)
Infostructure	The critical mass of protected information and information processing capabilities, trained personnel, and assured connectivity so warfighters, and

	warfare supporters can gain hands-on experience with the power of information and the possibilities of networking. (SECDEF Annual Report 2000)
Infrastructure	The underlying base or foundation especially for an organization or a system. The basic facilities, services and installations needed for the functioning of a community or society. (American Heritage Dictionary of the English Language, 1996)
Intelligence Community	The departments, agencies and activities enumerated in Section 3 of the National Security Act of 1947, as amended 50 USC 401a. Includes the CIA, NSC and DIA.
Interoperability	The ability of different organizations and systems to share and utilize information.
Investment Management	Management of the commitment of financial resources including capital planning, finance management, program management, procurement, and financial aspects of acquisition.
Joint Community	The directorates on the Joint Staff, the combatant commands, and joint activities that are responsible to the Chairman of the Joint Chiefs of Staff.
Human Capital	Personnel trained to perform required duties and assume authority and take responsibility.
Human Resources	Personnel, training, organizations.
Key Performance Parameters	Those capabilities or characteristics considered most essential for successful mission accomplishment. Failure to meet an ORD KPP threshold can be a cause for the concept of system selection to be reevaluated, or the program to be reassessed or terminated. Failure to meet a CRD KPP threshold can be a cause for the family-of-systems or system-of-systems concept to be reassessed, or the contributions of the individual systems to be reassessed. KPPs are validated by the JROC.
Knowledge	Acquaintance with facts, truths, or principles, as from study or investigation; familiarity or conversance, as with a subject, language, or branch of learning; acquaintance with a thing, place, person, as by sight, experience, or report; the fact or state of knowing; perception of fact or truth; clear and certain mental apprehension; the state of being cognizant or aware. [Webster's].
Knowledge (In the context of the ICF)	Information content and relationships within their scope and context along with rules as they apply to various situations as trusted by the holder.
Knowledge Presentation Framework	A paradigm that describes the assembly of raw data into usable views, documents, and decision support workspaces that can be used as "knowledge."
Meta-View	A "view of views" which provides the knowledge worker with an indication of what knowledge products have been created so that they can be used or combined to create new knowledge objects, or views. It would be an index of views that indicates how the views can be used.

Mobile User Environment	Computer and communication resources that a user requires to communicate, process and collaborate while on the move.
National Security Systems	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which - (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons system; (5) is critical to the direct fulfillment of military or intelligence missions. They do not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).
Operational Architecture	A description of the tasks and activities, operational elements and information flows required to accomplish or support an operation - whether the operation is military or combat support. (DoD C4ISR Architecture Framework)
Operations Requirements' Document	A formatted statement containing performance and related operational parameters for the proposed concept or system. Prepared by the user or user's representative at each milestone beginning with Milestone I.
Policy	A plan, course of action intended to influence and determine decisions, actions and other matters. A course of action, guiding principle or procedure considered to be expedient, prudent or advantageous. (Derived from American Heritage Dictionary of the English Language, 1996)
Revolution in Business Affairs	The willingness to abandon traditional processes in order to do things more quickly and cheaper. It results in a dramatic change in acquisition, logistics and business-management practices. (www.navyleague.org/seapower/revolution_in_business_affairs.htm 19NOV00)
Revolution in Military Affairs	The dramatically rapid evolution of weapons, military organizations, and operational concepts made possible by advancing technology. (Galdi, White paper, Revolution in Military Affairs? 11DEC95, www.fas.org/man/crs/95-1170.htm (19NOV00))
Rules	A generalized statement that describes what is true in most or all cases. An authoritative, prescribed direction for conduct. (Derived from American Heritage Dictionary of the English Language, 1996)
Seamless	Without seams. Connecting points are not noticeable. Perfectly consistent.
Span of Control	Amount of an organization or entity that one can effectively manage.
Strategic Vision	A broad and profound future situation that defines the direction of an organization.
System Administrator	Manager who is responsible for the operations, maintenance and configuration of an information system.
System Architecture	A description, including graphics, of systems and interconnections providing

	for or supporting warfighting functions. (JTA)
Team User Environment	Workstations, large screen displays, teleconferencing equipment peripherals, operating system, software, configurations and connections that provide a standardized set of communication and computing resources to connect a conference room or group to Information, Application and Collaboration Services.
Technical Architecture	A minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements that together may be used to form a system and whose purpose is to insure that a conformant system satisfies a specified set of requirements. (JTA)
Theater Information Grid	Theater components of the GIG.
Understanding	The ability or power to acquire and interpret knowledge; comprehension; intelligence; mental faculties or power of discernment; personal interpretation; knowledge of a particular field; ability to cope or deal with something.
View	In the context of the Knowledge Presentation Framework, it is the standard way of pulling together elements of knowledge for presentation. A view can be a simple display slide, a template connected to live data, a video feed and the like. Views can be combined to form new views or Decision Support Workspaces.
Wisdom	The faculty to discern right and truth and to judge or act accordingly; sound judgment, sagacity, discretion, common sense, extensive knowledge. [Webster's] (An innately human trait not to be associated with computers or computing.)

APPENDIX C- REFERENCES

Cohen, William S., Secretary of Defense, Document, Annual Report to the President and Congress - 2000, 1 January 2000, U.S. Government Printing Office, Washington, D.C.

Shelton, Henry H., Chairman of the Joint Chiefs of Staff, Joint Vision 2020, Office of Primary Responsibility: Director for Strategic Plans and Policy, J5, Strategy Division; June 2000, U.S. Government Printing Office, Washington, D.C.

Blair, Dennis C., Commander-in-Chief, U.S. Pacific Command, Remarks at the Armed Forces Communication and Electronics Association (AFCEA) Western Conference - 2001, 23 January 2001, San Diego Convention Center, San Diego, CA

Blair, Dennis C., Commander-in-Chief, U.S. Pacific Command, Pacific Command Mission Briefing, 2 October 2001, U.S. Pacific Command Headquarters, Camp H.M. Smith, HI

Cieslak, Randall C., Chief Information Officer, U.S. Pacific Command, U.S. Pacific Command Chief Information Officer Concept of Operations, 30 March 2001, U.S. Pacific Command Headquarters, Camp H. M. Smith, HI

Cieslak, Randall C., Chief Information Officer, U.S. Pacific Command, White Paper, An End-to-End Capabilities-Based Approach to Implementing Information Systems, 22 December 1998, U.S. Pacific Command Headquarters, Camp H.M. Smith, HI

Hyten, John, Lt Col, USAF, Joint Staff J-38, Interoperability and Space Operations Division, Briefing Presentation, Joint Operational Architecture (JOA) and Joint Mission Areas (JMAs), June 2000, Joint Staff, Pentagon, Washington, D.C.
<http://www.hq.pacom.smil.mil/c2s2_sh/j552/visits/000615_JWCA/Briefs/JOA-JMA.ppt> 2 Oct 01

Money, Arthur; DoD Chief Information Officer, Memorandum, Global Information Grid (GIG), 22 September 1999, Office of the Secretary of Defense, Pentagon, Washington, D.C.

Director, Defense Information Systems Agency (DISA), Defense Information Infrastructure (DII) Master Plan, 28 July 1995, DISA Headquarters, Arlington, VA

Reilley, Michael, Space and Naval Warfare Systems Center San Diego (SSC SD), Briefing Slide, "DoD/IC Technology Architecture" extracted from the Intelligence Collaboration Operational Network (ICON) 13 October 1999, SSC SD, San Diego, CA

Hammond, Naval Facilities Command, Briefing Slide: "Integrated Facilities Process Model" extracted from the brief: NAVFAC CIO Update to DON CIO Data Management, 25 August 1999, Navy Memorial, Washington, D.C.

Andrew, Thomas L., Col. USAF, Commander, Joint Interoperability Test Command (JITC), Defense Information Systems Agency (DISA), Joint Operational Networks, Status of Interoperability Report for the Theater Missile Defense Family of Systems, 17 September 1999, DISA JITC, Fort Huachuca, AZ, <<http://barbados.jitc.disa.smil.mil/tstrpt/tmd/sirsep99.htm>> 2 Oct 01

Porter, Daniel, Department of the Navy Chief Information Officer, Information Technology Standards Guidance, Release 98-1.1, 15 June 1998, Department of the Navy, Pentagon, Washington, DC

Hicks, Janet A., Director, Command, Control, Communications, Computer Systems, U.S. Pacific Command, U.S. Pacific Command Network Operations (NETOPS) Concept of Operations, 9 April 2001, U.S. Pacific Command Headquarters, Camp H.M. Smith, HI

Valetta, Anthony M., Assistant Secretary of Defense for Command, Control, Communication and Intelligence Systems (ASD C3I), and the C4ISR Architecture Working Group, C4ISR Architecture Framework Version 2.0, 18 December 1997. Office of the Secretary of Defense, Pentagon, Washington, DC <http://www.c3i.osd.mil/org/cio/i3/AWG_Digital_Library/pdfdocs/fw.pdf> 2 October 2001

Department of Defense Directive 5200.28, Security Requirements for Automated Information Systems (AISs), 21 March 1988, Office of the Secretary of Defense, Pentagon, Washington, D.C.

Department of Defense Manual, 5200.40-M, Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Document, 21 April 1999, Office of the Secretary of Defense, Pentagon, Washington, DC

Money, Arthur, Department of Defense Chief Information Officer, Guidance and Policy Memorandum, Department of Defense Global Information Grid (GIG) Information Assurance, 16 June 2000, Office of the Secretary of Defense, Pentagon, Washington, DC

Mansfield, Terry, LTC, U.S. Army, C4 Plans, Policy and Projects Division, U.S. Joint Forces Command, J61, Capstone Requirements Document, Global Information Grid, JROCM 134-01, 30 August 2001, Commander-in-Chief, Joint Forces Command, Norfolk, VA

APPENDIX D- ACKNOWLEDGEMENTS

The USPACOM CIO wishes to thank the following people who contributed their time and talent into creating the ICF. The USCINCPAC CIO assumes full responsibility for the content and quality of the document, particularly any shortcomings or errors. The following people provided excellent enhancements that will allow the ICF to foster creation of coherent Infostructure architectures and implementation plans.

Name	Title	Organization	Staff Code	Contribution
Dick Griffin	Mr.	SSC SD	J01CX	Writer/Editor
Dave Hunninghake	Lt Col, USAF	USCINCPAC HQ	J01C5	Concept/Editor
Joyce Jenkins-Harden	Lt Col, USAF	USCINCPAC HQ	J65	Concept/Editor/Staffing
Jens Jensen	Mr.	USCINCPAC HQ	J30/OPT	Concept
Byron Leong	Mr.	MITRE	J01C52	Writer/Editor/ Staffing
Art Nakagawa	Mr.	SSC SD	J644	Concept/Editor
Barbara Pierce	Ms.	USCINCPAC HQ	J01CA	Writer/Editor/ Staffing/ Production
Steve Ptak	MAJ, USA	USCINCPAC HQ	J30/OPT	Concept/Editor
Mike Reilley	Mr.	SSC SD	J006	Concept
Sig Runge	Mr.	Booz Allen Hamilton	J01C55	Editor
Toi Screnci	Lt Col, USAF	USCINCPAC HQ	J644	Concept/Editor
George Sowell	Lt Col, USAF	USCINCPAC HQ	J01C5	Concept/Editor
Melanie Winters	Ms.	Booz Allen Hamilton	J01C4	Writer/Editor

APPENDIX E- FIGURES

Figure 1. Using The ICF To Bridge The Understanding Gap Between Information Professionals, Operational Users and Program Managers3

Figure 2. Information Capabilities Framework High-Level Organization 3

Figure 3. Information Capabilities Framework High-Level Depiction of Theater Information Status.....4

Figure 4. Illustration of the Infostructure.....8

Figure 5. Using Capabilities Scope to Manage Interdependencies.....11

Figure 6. Comparison of the ICF to the Seven Layer OSI Model.....11

Figure 7. Terms Used in DoD to Describe the 'Infostructure'12

Figure 8. Using the ICF to Depict System Status Trends.....13

Figure 9. Using the ICF to Support System Implementation.....14

Figure 10. Using the ICF to Support DOTMLPF Planning.....15

Figure 11. Using the ICF to Support Investment Management.....16

Figure 12. Using the ICF to Perform System Integration Management.....16

Figure 13. ICF Relationship to the GIG CRD 17

Figure 14. GIG CRD Categories Captured Within the USPACOM ICF.....18

Figure 15. Illustration of the Application Layer Using the Information Layer as the Hub.....19

Figure 16. Infostructure in System Integration Management Format.....20

Figure 17. Infostructure in System Integration Management (SIM) Format for a Joint HQ Staff.....20

Figure 18. User's View of the Infostructure.....22

Figure 19. System Manager's Perspective of the Information Infrastructure.....22

Figure 20. Using the ICF to Support Creation fo System Architectures.....23

Figure 21. Showing System Footprints on the ICF Architecture.....24

Figure 22. ICF Support of the USCINCPAC New Headquarters24