3.0 DIS TARGET ARCHITECTURE PERSPECTIVES AND EVOLUTION

This section summarizes the DIS target architecture perspectives and evolution. The DIS target architecture provides a consistent structure for distributed information management across the entire DoD. The objectives of the DIS target architecture are cost reduction, greater efficiency, greater mission effectiveness, interoperability, and consistent security.

The TAFIM is being promulgated by the Office of the Secretary of Defense (OSD). It mandates the use of open systems, software reuse, and data management, communication, and security standards to achieve significant DoD cost reduction, interoperability, and security for all defense mission areas. *The TAFIM is the DIS target architecture.*

The DGSA describes the security perspective of the DIS. The DGSA will become a separate volume of the TAFIM, and will later become integrated with portions of the TAFIM volumes. *The DGSA is the DIS target security architecture.*

The DIS target architecture is composed of mission information systems and the DISN. The completed DIS target architecture is the TAFIM with the integrated DGSA and DISN architecture guidance documents, which will be applied to and support the specific architectures of mission information systems.

The requirements drivers for the TAFIM, the DGSA, mission information systems, and the DISN are set by elements of the DoD hierarchy. These requirements drivers form the basis for all programs and joint initiatives within the DoD that develop specific applications for information management. The TAFIM Information Management (IM) Integration Model organizes the DoD hierarchy into five levels (enterprise, mission, function, application, and personal), which are described in section 3.1.2. The Integration Model provides a basis for assigning IM integration responsibilities by making explicit the intersections of functions that can be categorized and assigned management responsibilities. Thus, requirements at all levels of the TAFIM IM Integration Model are considered in the DIS target architecture and are combined to drive major application development programs and joint initiatives. Major program and joint initiative application requirements, which are used to develop specific architectures, are therefore consistent when specific architecture development is guided by the generic DIS target architecture. These requirements interrelationships are not accidental. A coordinated, consistent, orderly, and effective DIS evolution cannot be realized without this interrelated means of expressing requirements.

Open system standards are a major element of the DIS target architecture. Many of the security requirements, discussed in section 2, are directly attributable to the open systems mandate. Requirements for compliance with standards are pertinent to all levels of the TAFIM IM Integration Model. Only in special cases will exceptions be made to specific standards applicable to a mission area (e.g., in tactical systems, which in limited cases may have unique standards).

Time constraints, the state of technology, budget limitations, and backward compatibility act as limitations to achieving the DIS target architecture. Therefore, *transition strategies* are necessary. Some requirements that drive the DIS target architecture cannot be achieved by any specific date. Such requirements are categorized as *far term*. Similarly, many mission, function, or application requirements will be in this same category. Many transition strategies (categorized by estimated timeframes) will be developed to achieve the realization of the DIS target architecture in evolutionary phases. Specific mission, function, or application programs will be expected to develop transition strategies that establish a planned evolution consistent with DIS target architecture transition phases. The DIS target architecture evolution is discussed in section 3.3.

Figure 3-1 illustrates the objectives, guidance, relevance, and some example implementation and integration programs that are building blocks in the evolving DIS target architecture.

Figure 3-1. Building Blocks of the DIS

3.1 TAFIM GUIDANCE

The TAFIM is composed of several volumes. For the purpose of synopsis and correlation with the DGSA, TAFIM volume 2 has served as the reference. The TAFIM cites two concepts that apply to the DIS security architecture the DoD Technical Reference Model (section 3.1.1), and the TAFIM IM integration model (section 3.1.2).

3.1.1 DoD Technical Reference Model

The detailed DoD Technical Reference Model (TRM) is illustrated in figure

3-2. The application layers are delineated based on their mission-specific and general-purpose use. The *mission area applications layer* pertains to those applications tailored to specific mission needs (e.g., decision aids, battle management applications, imagery processing applications, message and signals processing applications). The mission area applications may make use of general support applications. The *support applications layer* provides generic services, common to multiple mission areas (e.g., word processing, spreadsheets, Graphical User Interface applications, database query language application, network services applications).

The *application platform layer* provides the common information processing and communications functions used in general-purpose and multimedia information management processing environments. A platform is composed of one or more processors, operating systems, kernel functions to support the operating system, and peripheral External Environment Interfaces (EEIs) controlled by the kernel functions for devices such as terminals, printers, and storage devices. The application platform layer also includes Open System Environment (OSE) programming services, user interface services, data management services, data interchange services, graphics services, and network services provided to mission-specific and support applications through Application Program Interfaces (APIs). APIs provide the standard interfaces between mission and support applications, and between support applications and the platform's operating system, which may extend to applications on other platforms using the network services and the kernel-controlled EEIs used to interface to communication networks. The network services provide the communication protocol stacks in the platform necessary to communicate, end-to-end, between support or mission-specific applications. The network services applications may include support for data, voice, video, and imagery (e.g., facsimile).

Figure 3-2. DoD Technical Reference Model

The *external environment layer* provides the external communication services necessary to provide platform-to-platform (information system-to-information system), and subsequently application-to-application services, across communication networks. External communications (the communications infrastructure) are composed of local level (e.g., base level) networks, and wide area, regional or metropolitan area (e.g., support for several bases or tactical assets), and global networks. The external environment layer also provides information services and human or computer interaction services for the platform to interact with local information interchange devices (e.g., peripherals) and with users. The external environment interfaces will be compliant with existing and future standards.

3.1.2 TAFIM Information Management Integration Model

The TAFIM IM Integration Model provides a basis for assigning IM integration responsibilities. This model makes explicit intersections of functions that can be categorized and assigned management responsibilities. This model is illustrated in figure 3-3.

Requirements established by a higher authority are inherited (must be adhered to) by the lower levels, and are expanded at each of the lower levels to meet specific operational requirements. Integration issues between levels must be addressed. Except at the enterprise and the personal levels, integration issues also must be addressed among the components within each level.

The *enterprise level* includes those elements of information management that are mandatory across the entire DoD. Elements such as policy and doctrine are established by both OSD and the Joint Staff that apply across all DoD missions. Such policy and doctrine also may be mandated by a higher authority, such as presidential executive orders and national decision directives, Office of Management and Budget (OMB) circulars, and public law. The enterprise level also promotes information technology (e.g., technical and data standards), reference models and technical architectures, methods and tools, and shared computing and telecommunications services. The TAFIM, the Defense Information Infrastructure (DII), and the DGSA are all elements of the enterprise-wide level that combine to provide IM guidance and direction in support of DoD-wide missions.

The *mission level* includes those elements of IM that are mandatory across an entire mission area, and coordinates those elements of IM that are required for inter-mission needs. The mission level is responsible for defining mission-specific functional areas (described below) necessary to fulfill the operational requirements developed to conduct and support the mission. The mission areas defined by the TAFIM are Business, Command and Control (C2), and Intelligence. The purpose of the DIS is to support the needs of all of these DoD mission areas. From this IM perspective, C4IFTW is a mission area guidance focus for C2.

Figure 3-3. TAFIM IM Integration Model

At the *function level,* mission areas are refined into functional areas. Functional areas are generally categorized by the roles and responsibilities a particular organization or group of organizations perform to fulfill particular areas of the mission. From an information management perspective, a functional area includes those information services necessary to fulfill the specific functional areas of the mission. It is possible that functional areas of different missions may be of use in other missions. In these instances, common functional areas may be created to cross mission boundaries.

The *application level* includes the development, maintenance, and operation of the information system applications that provide required automation support to mission area functions. Integration at this level encompasses system interoperability, data sharing, and other technical issues that enable the efficient operation of information services. Integration at the boundary between the application level and the function level includes access to subject-matter databases and other system functions. The DMS is an application level program implemented to support functional areas of all missions. The DMS Target Architecture and Implementation Strategy, as a DoD-wide application level architecture and strategy, is coordinated at the enterprise level and provided to all mission and functional areas of DoD as its common secure messaging system application service, accommodating both individual and organizational message exchange needs.

The *personal level* addresses user support requirements that involve integration with the application level, while preserving privacy, individual choice, and personal preference at the desktop and workstation. Integration factors include stability and consistency of the human-machine interface to enhance personal productivity by insulating the user from the unique characteristics of individual systems at the system application level.

3.2 C4IFTW GUIDANCE

"The C4I for the Warrior concept will give the battlefield commander access to all information needed to win in war and will provide the information when, where, and how the commander wants it." (Powell, 1992)

The C4IFTW concept is both a vision and a road map to tactical C4I modernization. It provides the structure within which a unified, joint force structure will meet its information management and communications needs to fight wars and low-intensity conflicts effectively. Although each of the Military Services currently has its own unique C4I modernization efforts under way, C4IFTW imposes mandates for interoperability and shared resources on each of the Service-unique architectures.

The C4IFTW concept identifies three distinct phases. The first is a *quick-fix phase,* which provides translators, gateways, and joint standards to achieve quick-reaction (but not necessarily efficient) interoperability. The second phase, called the *mid-term phase*, provides modular building blocks and total interoperability for new C4I systems, and a jointly shared wide area network. The third phase, called the *objective phase*, provides evolving and advanced technologies identified and assimilated for the war fighter. This phase also provides a standardized interface environment and a global C4I network of fused information for complete requirements realization.

The quick fix phase only partially maps to the TAFIM because of the existence of legacy systems. The mid-term phase maps conceptually to the TAFIM in the perspective of transitioning toward the DIS target architecture. The objective phase maps directly to the TAFIM and reflects the realized DIS target architecture. The complete range of MLS requirements postulated by C4I tactical operations only can be achieved through the employment of the DGSA (i.e., requirements expressing the need to accommodate unclassified through Top Secret/Sensitive Compartmented Information).

3.3 DIS TARGET ARCHITECTURE EVOLUTION

The development of the DIS will be evolutionary, but is required to be consistent with the TAFIM enterprise level mandates. The most abstract representation of the DIS is that of user elements connected to one another via local communications networks, which in turn have access to wide area communications networks. The wide area communications networks are, and will continue to be, DoD-owned (e.g., DoD-owned Military Satellite Communications resources), common carrier (U.S. and foreign) leased, and non-satellite radio frequencies. Commercial carrier services will be used to a much greater degree for both the tactical and non-tactical C4I network infrastructure over time. Eventually, it will no longer be prudent or practical from a cost perspective for DoD to own vast wide area communication resources, although some will have to be retained for survivability and to meet special requirements. User elements and their local communications may be fixed or mobile. The DIS target architecture, reflecting user elements and local and wide area networks, is illustrated in figure 3-4.

It must be understood that information systems are not restricted to computers and computer networks. Although exceptions apply to what follows, the intent is to be as widely inclusive as possible in considering applications and environments, while preserving significant freedom for architects and implementors of specific information systems. In particular, the following considerations apply to information systems in the DGSA.

3.3.1 Voice-Video/Imagery-Data

While the bandwidth, flow characteristics, error susceptibilities, and human interfaces to these media types may be different, they can be represented as bits of information and, therefore, are accommodated by digitally based processing and telecommunications.

Figure 3-4. DIS Target Architecture

3.3.2 Portable-Mobile-Fixed

Physical portability and mobility are achieved through efficient packaging, low-power design, and transmission media independence. It is assumed that bit integrity will be inherent in the communications networks used and that residual errors will be the responsibility of user systems components (as part of availability services). Likewise, naming and addressing issues are assumed to be solved in the context of open systems communications. Security mechanisms such as authentication and cryptography are required to support portable and mobile information systems.

3.3.3 Secure-Nonsecure

The requirement for open systems demands the compatibility of secure and nonsecure information systems. The DGSA is based on the expectation that the integration of secure and nonsecure components will be necessary to achieve the desired degree of protection, and that products will be developed, with varying degrees of protection, that will operate in open systems.

3.3.4 Workstations-Servers-Hosts

Automated information systems will require relatively minor hardware changes, but significant operating system, support software, and application software changes will be needed to achieve security as envisioned in the DGSA.

3.3.5 Programmable-Nonprogrammable

Weapons systems, sensors, and other remotely controlled devices will have custom interfaces and high demands for communications availability, but they can be made to fit well into information systems architectures. The security, as well as the operation, of unmanned objects that may be lost or destroyed needs careful consideration in implementation. Nonprogrammable devices need careful consideration in terms of their security life cycle but are otherwise not a factor in the DGSA.