THE DEFENSE MESSAGE SYSTEM

Robert W. Shirey

The MITRE Corporation, Mail Stop Z269
7525 Colshire Drive, McLean, Virginia 22102-3481
703.883.7210, shirey@mitre.org

ABSTRACT

The U.S. Department of Defense (DoD) plans to modernize the Defense Message System (DMS) to reduce costs and improve services. DMS includes all hardware, software, procedures, standards, facilities, and personnel used to exchange messages electronically in DoD. DMS today has two separate parts. The AUTODIN system handles formal messages between organizations, and the Defense Data Network's electronic mail system handles other messages. The DMS plan has a target architecture, for the year 2008, that integrates those separate systems, uses CCITT X.400 message handling and X.500 directory services, and provides writer-to-reader security with the Secure Data Network System developed by the National Security Agency. The implementation strategy has three phases that extend over 20 years. The plan has an indirect but strong effect on the Internet outside DoD.

1. INTRODUCTION

The DMS is defined as all hardware, software, procedures, standards, facilities, and personnel used to exchange messages electronically among organizations and individuals in the U.S. Department of Defense (DoD). Today's DMS is expensive to run, needs a large staff, and has service deficiencies. Budget limits and rapid advances in message handling technology are accelerating DoD's need to change DMS.

In January 1988, DoD's military services and defense agencies formed a working group to plan the future of message handling. The first goal was to reduce staff levels and other costs while maintaining the existing levels of service and security. The second goal was to improve service and security. Using industry inputs [1], the group outlined a new architecture and transition phases to achieve it. The DMS Target Architecture and Implementation Strategy (TAIS) [2] extends to the year 2008. It stresses standards and interoperability, but preserves adaptability for implementing unique functions and features needed by particular DoD organizations. The plan was approved by DoD's senior acquisition managers, and guidance was issued to establish the DMS Program and formalize its management structure.

The rest of this paper is organized as follows. Section 2 defines the two classes of DMS messages and identifies the two existing baseline systems that handle these classes. Section 3 and 4 state the functional requirements and architectural guidelines that the the military Joint Staff has established to guide the DMS evolution. Section 5 describes the elements of the two baseline systems, outlines how each system handles messages, and compares the systems to the requirements. Section 6 outlines the target architecture that is described in the TAIS. Section 7 summarizes the three-phase implementation schedule, outlines how the DMS program is managed, and tells where industry can get further information.

2. SERVICE CLASSES

A DMS message is either organizational or individual. This message service class is chosen by the originator, who acts according to DoD policy. Today's DMS has a major, separate system for each class, and the the systems are not interoperable. The TAIS will integrate them.

Organizational messages are command and control communications and other formal exchanges between organizations. They need release approval by officials of the sending organization, and there are rules for their distribution in the receiving organization. Organizational messages are handled by the Automatic Digital Network (AUTODIN) [3]. As seen by the writer and reader using AUTODIN, methods for organizational messages have changed little since World War II. AUTODIN's formality has resisted changes in formats, procedures, and interfaces. Upgrades have been made to improve support of existing practices, but not to aggressively exploit advances in technology and standards. The resulting system, while generally quite reliable and secure, does not give optimum service to its users, sometimes becomes overloaded, and is too expensive. AUTODIN operation and maintenance take over $1,000,000,000 (a billion U.S. dollars) per year and more than 20,000 staff positions. Much equipment is obsolete. (Punched paper tape and cards are still used.) Service from writer to reader is too slow because of manual methods of preparation and delivery.

Individual messages are working communications between persons within administrative channels, but such messages do not usually commit or direct an organization. Most individual messages are sent as internetwork electronic mail [4] on the Defense Data Network (DDN) wide area networks (WANs) and

their connected local area networks (LANs) [5]. Compared to AUTODIN, this mail service is modern, fast, flexible, and less expensive; but it has no service standards. It lacks assured reliability, accountability, and other attributes needed by DoD. Still, the growth of DoD data networks led to such widespread use of internetwork mail that DoD policies for its use became necessary. Current policy separates internetwork mail from AUTODIN communications. Commanders may formalize that mail within their own commands, but between commands it is normally considered informal.

3. FUNCTIONAL REQUIREMENTS

The Joint Staff has "validated" (i.e., formally established) the DMS requirements:

- Connectivity. DMS must serve all DoD component organizations and individuals, offer access to and from all DoD locations worldwide, and interface to other U.S. government, allied, tactical, and contractor systems as needed.

- Guaranteed delivery. DMS must deliver messages with a high degree of certainty, and maintain writer-to-reader accountability.

- Timely delivery. DMS must preferentially handle critical information during peacetime, crisis, war, and periods of system stress.

- Confidentiality. DMS must handle information of all DoD classification levels and compartments, protecting it from unauthorized disclosure.

- Sender authentication. DMS must verify the source of a message and ensure authorized release of organizational messages.

- Integrity. DMS must ensure that the information content of a message is not changed.

- Survivability. DMS must be as survivable as its users, and be capable of reconstitution.

- Availability. DMS must be highly reliable and available, and serve users around-the-clock.

- Ease of use. DMS must be usable without extensive, specialized training.

- Identification of recipients. DMS must have accurate directories that enable the originator to unambiguously identify the intended recipients.

- Message preparation. DMS must be very user-friendly.

- Storage and retrieval. DMS must store messages after initial delivery to allow retrieval for resending and for automated archiving, analysis, and editing.

- Distribution determination and delivery. DMS must deliver an organizational message according to requirements of the intended recipient. DMS must deliver an individual message to the individuals specified by the originator.

4. ARCHITECTURAL GUIDELINES

The Joint Staff has also established seven architectural guidelines for DMS:

- Computer communication protocol standards. DMS will migrate to the Government Open Systems Interconnection Profile (GOSIP) [6]. GOSIP is the U.S. government specification for implementing international standards based on the seven-layer Open System Interconnection (OSI) model [7]. This guideline affects the DMS subsystems differently. AUTODIN has unique protocols that are not layered; it has no easy way to evolve. This guideline means that AUTODIN components must be phased out and physically replaced. The DoD internetworks use the same protocol standards as the larger, non-DoD Internet does [8]. These public protocols are layered similarly to OSI, and evolution will be easier. However, this will cause a large ripple effect in the Internet because of interoperability requirements and changes in the equipment market.

- Nondevelopmental items (NDI) and services. DMS will use commercially available, off-the-shelf components whenever possible.

- Commodity purchases. DMS will use standard, competitively acquired, general-purpose computers to minimize cost and maximize commonalty, interoperability, and evolutionary potential.

- Portable operating system interface (POSIX). DMS will use the nonproprietary POSIX interface for operating systems [9], to provide a standard, hardware-independent base for software.

- Standard computer languages. DMS will use the Ada programming language for DoD developments [10].

- Commercial COMSEC endorsement program (CCEP). DMS will use the National Security Agency's (NSA) integrated CCEP products and designs where needed to meet security requirements [11].

- Computer security certification. DMS will apply the Trusted Computer System Evaluation Criteria (TCSEC) [12] to the maximum extent possible consistent with the objective of minimizing new developments and life cycle costs and maximizing the implementation of NDI components.

5. BASELINE

The baseline systems are AUTODIN and DDN-based internetwork mail. This section describes their components and outlines how they handle a message. The operations described here are the classical ones; actual operations vary at many system sites. Many details are omitted here, and some actions described as manual are sometimes automated. The baseline systems have surface similarities but are basically quite different. AUTODIN uses a closed, special-purpose, store-and-forward message-switching network dedicated to handling organizational messages. DDN internetwork mail shares an open, general-purpose, packet-switching network that supports other applications besides mail. AUTODIN's backbone structure is static. DDN

is growing and evolving, and the Internet to which DDN's unclassified segment (MILNET) connects is growing very rapidly. Neither AUTODIN nor DDN internetwork mail meets all the validated requirements and guidelines listed in Sections 3 and 4.

5.1 AUTODIN Backbone and Relay Structure

AUTODIN includes all the elements involved in providing worldwide message service between DoD organizations. The backbone has 15 AUTODIN switching centers (ASCs) and 76 interswitch trunk (IST) lines. Each month, the backbone handles around 50 million messages, which average about 3,000 characters. The Defense Communications Agency (DCA) manages the backbone from three operation centers (OCs) in the continental U.S. (CONUS), Europe, and the Pacific. The CONUS OC has a mainframe computer that connects to AUTODIN and receives status and performance reports in message form from ASCs, but DCA controllers send commands to ASC sites via orderwire or telephone, not through AUTODIN. OCs resolve problems that affect multiple ASCs. Problems that affect only a single ASC or its subscribers are handled by the ASC site.

An AUTODIN subscriber is a physical device that originates or receives messages. A device may serve one or more organizations. A device that connects to an ASC is a direct subscriber. All ASCs together have about 1,400 direct subscribers, ranging from teletypewriters to large computers. Some direct subscribers are message relays, and about 70 are major relays called automated message processing exchanges (AMPEs). An AMPE relays and routes messages between back-side connections and the backbone. A device that connects to a relay is an indirect subscriber. All together, about 600 indirect subscribers connect to the back side of AMPEs. Some indirect subscribers are secondary relays that allow other devices to connect through various means, including LANs, and over various distances. In OSI terms, the ASCs, AMPEs, other relays, and many subscriber devices are all end systems that implement the functions of all seven layers; but they use protocols that are much older than OSI or Internet standards.

A subscriber device is usually also an AUTODIN terminal, which is a logical end point of the system; AUTODIN's formal responsibility for a message begins or ends there. A terminal is usually located in a telecommunications center (TCC) or data processing installation (DPI). A terminal may originate messages, receive messages, or do both. An AMPE or other relay may also act as a terminal and provide over-the-counter message service. For messages addressed to a terminal, the formal rules associated with electronic processing of an AUTODIN message stop at the terminal. If a terminal outputs a message in human-readable paper form, other formal procedures may apply to the message until its ultimate delivery. However, the message may also be sent beyond the terminal point, in electronic or other form, without following AUTODIN rules or offering AUTODIN service assurances. Some terminals are automated message handling systems (AMHSs) that redistribute AUTODIN messages within communities of interest. Some terminals connect to LANs or WANs, and AUTODIN connects to radio networks to reach mobile users.

5.2 AUTODIN Message Handling Overview

AUTODIN message flow follows formal procedures. The originator composes a message off-line and types it on DoD Form 173 (Joint Message Form) in an optical character reader (OCR) font. For each intended recipient organization (e.g., the Director of DCA), the originator looks up the plain-language address (PLA) (e.g., "DCA WASHINGTON DC") in the Message Address Directory (MAD), a volume published quarterly on paper by the Military Communications Electronics Board (MCEB). A release authority for the organization signs the message form, which is carried to the local TCC.

A TCC terminal operator converts PLAs into routing indicators (RIs), the internal AUTODIN addresses (e.g., "RUEJDCA"), by looking up each PLA in Allied Communication Publication (ACP) 117, an MCEB paper publication, updated monthly. If the local terminal device connects through an AMPE, the AMPE does the conversion. AMPE tables are updated manually and frequently, from ACP 117 changes and other sources. A PLA may represent one RI, or may denote a locally or globally defined distribution list of prespecified addressees. The operator also assigns a locally unique date-time group and enters the originating station RI.

The message is read into the local subscriber terminal device by OCR, or is retyped in some cases. The terminal reformats the message according to military standards for organizational messages, and transmits the message using a protocol unique to AUTODIN. At the first AMPE or ASC en route, the first several lines of the message are validated. An AMPE makes local deliveries to terminals connected to it, and sends the message on to an ASC. An ASC makes local deliveries to terminals connected to it, and routes the message as needed to connected ASCs. One copy of the message is sent to each next ASC, along with only those RIs for which that next ASC is responsible. This process repeats until the message is delivered to all intended recipient terminals.

Formal procedures govern distribution and delivery. At a recipient terminal, multiple copies of the message may be made based on distribution lists (implied by office codes included by the originator as additions to the recipient organization's PLA), the subject matter of the message, content indicator codes, North Atlantic Treaty Organization (NATO) subject identifier codes, or the content of the message text itself. Reproduction and distribution may be manual or may be automated in the receiving AMPE or terminal, or in an attached AMHS. Paper copies are carried by hand to the actual recipients.

5.3 AUTODIN Compared to Validated Requirements

Graded against the requirements in Section 3, AUTODIN scores slightly over 50 percent.

Connectivity is good between some 70,000 commanders, but between lower organizational elements it depends on non-standard methods and is difficult. Guaranteed delivery is supported by redundancy but is hindered by manual processing errors at both ends. Timely delivery is assured for important messages by a priority (precedence) system and many special actions, but routine traffic may be seriously delayed. Confidentiality is adequate for all levels of classified information, but the TCSEC is unused. Sender authentication is marginal and depends on operators checking written signatures. Integrity is not end-to-end because ASCs and AMPEs alter and expand messages en route, and because conversions are supported between encoding schemes such as FIELDDATA and EBCDIC. Survivability is limited by having only 15 ASCs. Availability is high but costly, due to equipment redundancy and dedicated, on-site maintenance. Ease of use is not an AUTODIN characteristic; trained operators are needed for many functions. Identification of recipients is provided only by paper directories, and messages may not always be distributed to all interested parties at the destination. Preparation support is nonexistent except for local initiatives. Storage and retrieval support is provided in the backbone and in AMPEs, but only for resending; other support depends on AMHSs, which are not universally deployed. Distribution determination and delivery is automated at some AMPEs, TCCs, and AMHSs, but is limited by formats and standards.

5.4 DDN Backbone and Host Structure

Each DDN segment--the classified DSNETs and the unclassified MILNET--has its own, physically separate backbone. (By the early 1990s, the DSNETs will merge to form DISNET [13].) Each backbone has computers called packet-switching nodes (PSNs) connected by interswitch trunks (IST) lines. A DDN subscriber is an organization that uses DDN service. A subscriber gets full service by connecting an automated information system (AIS) to a PSN port via a dedicated host access line. An AIS connected to a PSN port is called a DDN host. Hosts typically support back-side, input-output devices called terminals. A terminal on a host can range from a teletypewriter to another mainframe. Hosts called internetwork routers connect the backbone to other WANs and LANs. In OSI terms, PSNs are intermediate systems that implement the three lower layers, and hosts are end systems that implement all seven layers.

Subscribers get a limited form of DDN service by connecting a terminal (which need not be intelligent) to the back side of one of the special-purpose, DCA-operated hosts called terminal access controllers (TACs). TACs offer both dedicated and dial-up connections. TAC service enables a terminal to communicate through the backbone to a second host, as if the terminal were connected directly to the second host.

Monitor center (MC) hosts at the DCA OCs receive status and performance information through the backbones from PSNs, TACs, and other devices. Unlike in AUTODIN, MCs also control the PSNs and other elements with commands sent through the backbone itself.

DDN is growing and evolving. At the end of September 1989, MILNET alone had 229 PSNs; 496 ISTs; 2,025 subscriber hosts connected and actively communicating packets across the network; and other special hosts, including 214 TACs supporting 3,613 dial-up and 1,324 dedicated terminal ports. DDN has been adding about 50 hosts per month. In October 1989, MILNET hosts sent 1.95 billion packets (1.9 billion originated in the CONUS) averaging 70 characters. It is estimated that 25 to 50 percent of these packets result from internetwork mail.

5.5 DDN-Based Internetwork Mail Overview

The originator uses a name and password to log in (from a dumb terminal or personal computer) as a user at a mail host, which usually is a general-purpose AIS that provides other services besides mail. The user interacts with application software to compose and send a message. For each intended recipient for which the user does not know the mail address, the user may enter a host command to request the address (but the user usually learns mail addresses some other way). The host responds with a mailbox address, which consists of a name for a mail host, plus a name for a user at that host (e.g., SMITH@DDN1.DCA.MIL). For this, the host may connect the user to another host that provides a directory that is similar to the telephone white pages. A partial white pages for MILNET is maintained by the DDN Network Information Center.

The originator enters a host command to compose a message. The host prompts the user for "TO" addresses, the subject, and the text. The host usually permits a "TO" address to be either a mailbox address or the name of a locally defined group (a distribution list) of addresses. When the message is complete, the user enters a command to send it. The host checks the message for proper text format [14] and adds fields for the "FROM" address, date, and time. The user may use local message and address formats, which the host converts to the Internet standards. The host converts distribution list names to lists of mailbox names. The host checks for correct host names (e.g., DDN1.DCA.MIL) in mailbox addresses, and converts the names to internetwork internal addresses (e.g., 26.4.0.106) [15]. If the mail host has not cached the names, it may communicate with a directory host.

The mail host then sends the message to each destination host mentioned in a recipient address. Only one copy of the message is usually sent to each destination host, even if the message is addressed to several mailboxes at the host. If an intended recipient host is unavailable, the originating host stores the message and attempts periodically to send it. After a time-out period, a notice and the unsent message are put in the originator's mailbox. A mail host sends messages using the DoD standard Simple Mail Transfer Protocol (SMTP) used throughout the Internet and

elsewhere [16]. DoD users can exchange mail with non-DoD users as permitted by physical connectivity, policy, and other factors.

A receiving mail host checks the names of the intended recipients against its list of users. If an intended recipient is a local user, the host puts the message in the recipient's mailbox. An intended recipient who is not a user on that host might be listed for forwarding to another host. If an intended recipient is not on either list, the originating host is notified, and it puts a non-delivery notice in the originator's mailbox. When a recipient user logs in at the receiving mail host, the host usually tells the user that mail has been received. The user typically can scan a list of message subjects and originator names (and on some systems, search the text and other fields for keywords) and either read, save, or erase messages. Some receiving hosts, if requested by the originator, may send a notification to the originating user when the message is sent to the recipient user's terminal. The recipient user may forward the message to other mailboxes on that host or other hosts. A user may keep some messages on file at a mail host for whatever purposes needed.

5.6 DDN Mail Compared to Validated Requirements

Graded against the requirements in Section 3, internetwork mail scores below 50 percent. Connectivity is possible among hundreds of thousands of mailboxes in MILNET and the rest of the Internet, but directory services and connections to tactical and commercial systems are inadequate. Guaranteed delivery is limited by lack of redundancy at most sites. However, host-to-host protocols include acknowledgements, and users can request acknowledgements from each other. Timely delivery depends on how often originating hosts send mail, how receiving hosts notify users, and how often users look at their mailbox. Actual host-to-host transmission takes only seconds. Confidentiality is limited except on DSNET segments, but the Internet community has just developed a new security system (which also offers sender authentication and integrity assurance) for unclassified mail [17]. Sender authentication is weak and depends on local host procedures. Integrity is good host-to-host, due to a reliable protocol, but often is poor on terminal-to-host access paths. Survivability is good because DDN is very decentralized. Availability is high for most hosts during normal business hours and conditions, but DoD has no standards for this. Ease of use is reasonable on most hosts, even for the new user, but could be greatly improved by more friendly software. Identification of recipients is limited by lack of white and yellow pages for DoD and by lack of standards for mailbox naming that would allow better guessing. Preparation support is universally provided on-line, but the degree and quality varies widely between hosts. Storage and retrieval support is similar to preparation support. Distribution determination and delivery responsibility is almost always a user function; mailing lists are extensively used but are typically not invoked automatically.

6. TARGET ARCHITECTURE

The TAIS describes a new, goal DMS that is fully automated from writer to reader and that integrates the handling of organizational and individual messages. The new message handling and directory systems use commercially available components based on international standards. Security services are based on products of NSA's Secure Data Network System (SDNS) program [18]. Data transmission is provided initially by the DDN MILNET and DISNET internetworks, and later by their successor systems which are referred to as the Defense Information System (DIS) and attached, base-level Installation Information Transfer Systems (IITS). The target architecture assumes the DIS and the IITS will be closely coupled and based on Integrated Services Digital Network (ISDN) technology [19].

A hierarchical, distributed set of management functions and components ensure effective DMS service by monitoring network status and performance, maintaining the directory, and controlling the system configurations.

6.1 The Message Handling System

The DMS TAIS adopts the CCITT X.400 model for its message handling system [20]. In the target system, an originator prepares messages with help from a user agent (UA) application process. A UA interacts with its message store (MS) or with the message transfer system (MTS), to submit messages on behalf of a user. The UA may perform additional functions defined locally to support message preparation, storage, retrieval, distribution, and delivery. A typical DMS UA is expected to run on a personal workstation or other small computer, along with other applications such as word processing and spreadsheet analysis.

The MTS consists of message transfer agents (MTAs) that operate as store-and-forward message switches. A UA can exchange messages directly with an MTA, or a UA can optionally use an MS as an intermediary between the UA and MTA. The MS stores received messages until the UA retrieves them, and it accepts submissions from the UA. MTAs and MSs probably will run on multitasked minicomputers.

An organizational user agent (OUA) is a UA that is augmented with application software to handle organizational messages. The OUA user can perform the message release authority function and approve organizational messages prepared by that UA or by subordinate UAs in that organization. The OUA assures that the user has the authority to release the message, or sends the message to an OUA with higher authority. The OUA can properly receive organizational messages, make the formal distribution determination, and deliver to subordinate UAs. The OUA can send messages of non-routine precedence, and can guarantee delivery when it receives such messages. The OUA maintains required message archives and ensures writer-to-reader accountability. Some OUAs may be specialized for these and other functions.

6.2 The Directory System

The TAIS adopts the CCITT X.500 model for its directory services [21]. The DMS directory is a set of open systems that cooperate to hold a database of information about DMS objects. The directory will be distributed along functional and organizational lines. Directory users (both people and computer processes such as UAs and MTAs) can read or modify the information if they have appropriate permission. A user accesses the directory information with the help of a directory user agent (DUA) application process. A UA will typically have a coresident DUA. The X.500 directory provides a well-defined set of basic services that the local DUA can use to provide the capabilities needed by a user. A DUA interacts with the directory by communicating with the set of directory service agent (DSA) application processes that collectively form the directory.

The DMS directory will support services needed to meet validated requirements. An originator will be able to use the directory to discover a potential recipient's capabilities--e.g., hours of operation, display capability, or storage capacity. An originator will be able to identify a recipient by user-friendly naming, which the directory will convert to the more complex, machine-oriented, X.400 originator/recipient (O/R) names and addresses. An originator will be able to address a message to a distribution list name, and the directory will provide the information to automatically expand that name. (In AUTODIN, globally defined and centrally maintained lists called collectives are used to support many military missions. There are hundreds of collectives, and some have hundreds of members.) All system elements will use directory information to implement access control and other security services.

6.3 The Security System

Message security services--data confidentiality, data integrity, data origin authentication, and (optionally) nonrepudiation with proof of origin (digital signature)--will be offered for both organizational and individual messages, and for both classified and unclassified messages. These services depend primarily on the SDNS Message Security Protocol (MSP) [22]. MSP is designed to be implemented in UAs and uses end-to-end, writer-to-reader encryption. An MSP gateway component will provide transitional interoperability between DMS UAs with MSP and those without, and will continue to provide interoperability with non-DMS UAs, including foreign military, commercial, and research communities. Other intra-DMS communication, such as between DUAs and DSAs, will be protected by a combination of other SDNS protocols and the security offered in the DIS and the IITSs. The SDNS Key Management Protocol will provide the basis for a DoD-wide system of DMS access control [23].

6.4 Operational Overview

This section sketches how the target system will handle organizational messages. Individual messages will be handled similarly, but without using the special capabilities of the OUA. A message will originate at a computer terminal, typically a personal computer, located in the user's own work area. Local procedures, computer login, and cryptographic features will authenticate that the user has organizational release authority, and will control access to other system privileges such as high precedence.

The OUA and other applications will have user-friendly screens, menus, prompting, and on-line error correction to help the originator prepare the message in a DMS Common Message Format, which will be a new ACP. The DUA will have similar features to help address the message. If the originator must coordinate the message with other users before releasing it, this may be done by passing the draft as an individual message, authenticated and signed using MSP, or by using local office automation or IITS features.

When completed, the message is released by the OUA user, authenticated and protected by MSP encryption, and sent by the OUA to an MTA, possibly via an MS. MTAs route the message using the intended recipients's O/R names and associated directory information. The final MTA sends the message either to the recipient OUA, or to an MS that either alerts the OUA that a message has arrived or takes other action depending on the message's precedence. The MSP protection is not decrypted until the message reaches the intended recipient's OUA. The OUA distributes an organizational message to the recipients specified by the originator and also to additional organization elements determined by local policies and procedures. Redistribution may be done using individual messages. Receiving users may read, print, store, analyze, or otherwise process the message.

The originating and receiving OUAs meet strict accountability requirements. They maintain audit information for security analysis, problem analysis, and other uses. They also provide long-term storage for retrieval, retransmission, and other reuse.

6.5 Target DMS Compared to Validated Requirements

Connectivity based on DIS and IITS networks will be universal throughout DoD and will be available to reach civil, tactical, allied, and commercial systems. Guaranteed delivery will be assured by a robust MTS and automatic methods of alternate delivery. Timely delivery will be assisted by precedence mechanisms, alternate delivery arrangements, and other automated features. In many organizations, of course, timely delivery will still require 24-hour-per-day staffing to assure that messages are read. Confidentiality, sender authentication, and integrity for messages, directory interactions, and other system elements will be assured by MSP and other SDNS mechanisms.

Survivability will depend on the underlying DIS and IITS. Ease of use will be enhanced by the new Common Message Format, automated aids at the user interface, and integration with the familiar information system used daily for other work. Identification and location of recipients will be supported by directory services and SDNS. Preparation support that is user-friendly and on-line will allow formatting and transmission of most messages with little training. Storage and retrieval support will be flexible and extendable, with standard minimum services. Distribution determination and delivery, primarily for organizational messages, will be automated and done according to local policy, using profiles based on message descriptors and attributes.

Overall, the target architecture is designed to reduce the cost of DMS. Competitive acquisition of commercially available components based on international standards should be less expensive than development of unique DoD components. Extending automation to the desk of the writer and reader should eliminate many manual tasks and support staff positions at TCCs and other AUTODIN locations. Replacement of obsolete and DoD-unique components by modern, standard, commercial components should increase reliability and otherwise reduce maintenance costs.

7. IMPLEMENTATION STRATEGY

The TAIS describes a three-phase plan for the transition from the 1989 baseline to the target architecture in 2008. All DMS elements--hardware and software components; policies and procedures; protocols, formats, and other standards; and user services--will evolve in multiple releases. DoD military services and defense agencies will include the TAIS in their plans, but will keep control of DMS components that must be tailored to accomplish unique local missions. The TAIS seeks near-term cost and staff reductions by early introduction of jointly-developed transition elements. New system elements will be tested in live user environments to prove their benefits before being widely deployed. Backward compatibility will support phased deployment of new elements, but the plan seeks to phase out obsolete elements quickly.

7.1 Implementation Phases

Phase 1 stresses projects to automate AUTODIN TCC functions and extend automated AUTODIN service to the user's desk. It also includes projects to field elements that will assist the transition to the new architecture. For example, the Message Conversion System (MCS) project will fully automate AUTODIN PLA-to-RI translation as a step toward the DMS directory service. The AUTODIN-to-DDN Interface (ADI) projects will connect and provide interoperability between AUTODIN and DDN. Application gateway projects will provide interoperability between SMTP and X.400 [24]. Many Phase 1 projects have already begun. When completed, they will enable DoD components to begin to reduce staff levels and other costs at bases and offices, migrate from AUTODIN to DDN, and convert to X.400/X.500. However, AUTODIN and DDN internetwork mail will still exist as separate systems at the beginning of Phase 2.

Phase 2 begins around 1995 with installation of the initial operational capability for X.400/X.500 individual and organizational message handling protected by SDNS MSP. During this phase, many TCCs, AMPEs, and ASCs will be closed. All AUTODIN users, and all SMTP users on DDN, will convert to being X.400 users on DDN.

Phase 3 begins around the year 2000, when the last ASC is closed. This phase will complete the integration of the two separate subsystems that exist today. Remnants of AUTODIN will be eliminated, as will transition elements such as ADIs. The DMS target components will evolve to use the integrated DIS and IITSs based on ISDN. Achievement of the target architecture is projected for the year 2008.

7.2 Management Structure and Industry Contact

The DMS Panel of DoD senior managers oversees the program, and the Implementation Group (DMSIG) coordinates plans and projects. The DCA DMS Coordination Division chairs the DMSIG, which has working groups for architecture, security, testing, and other areas. All DoD components participate.

In the TAIS, DMS is both a unified system of components working together to provide message handling service, and a composite of separate development and acquisition projects run by the individual DoD military services and defense agencies. Projects are categorized as central, joint, or user-unique. Central projects support the core architecture and all users; they involve backbone components or major policies and standards. Their funding receives high priority; and their development, testing, and deployment involve active participation of all services and agencies. Joint projects are individual service and agency projects that have the potential to meet the needs in other services and agencies and to advance the DMS architecture. Joint support for these projects reduces duplication of effort and promotes standardization. User-unique projects are carried out by a single service or agency to satisfy their special needs, but the projects still conform to DMS architectural standards. Joint projects have higher funding priority than user-unique projects, because joint projects have greater potential for cost reduction or other widespread benefits.

In summary, DMS is not a typical DoD acquisition program with fixed requirements, a fixed schedule, a single budget, and single program manager. Instead, DMS is evolutionary and has a joint DoD process to coordinate requirements, architecture, policies, standards, funding, and acquisitions.

The DCA DMS Coordination Division has publicly released the TAIS and will provide additional information as the program develops. A DMS Nondevelopmental Item (NDI) Demonstration Facility has been established and will begin operation in 1990. Information about this facility will be

given in the Commerce Business Daily. DMS information may be requested from DCA as noted below.*

REFERENCES

Some of these references are available from the following sources:

* Defense Communications Agency
DMS Coordination Division (Code DISM)
Washington, D.C. 20305-2000

** DDN Network Information Center
SRI International International
333 Ravenswood Avenue
Menlo Park, Calif. 94025

1. Defense Message System Request for Information, 21 January 1988.*

2. The Defense Message System (DMS) Target Architecture and Implementation Strategy (TAIS), December 1988.*

3. L. M. Paoletti, "AUTODIN", in R. L. Grimsdale and F. F. Kuo, ed's., Computer Communication Networks, Nordhoff, The Netherlands, 1975.

4. John S. Quarterman, The Matrix -- Computer Networks and Conferencing Systems Worldwide, Digital Press (Digital Equipment Corp.), 1990.

5. Heidi B. Heiden and Howard C. Duffield, "Defense Data Network", EASCON 82; 15th Annual Electronics and Aerospace Systems Conference, IEEE, New York, N.Y., 1982.

6. U.S. Department of Commerce, Government Open Systems Interconnection Profile (GOSIP), Federal Information Processing Standards Publication 146, 15 August 1988.

7. International Organization for Standardization [ISO], Information Processing Systems--Open Systems Interconnection Model--Basic Reference Model, International Standard 7498, Ref. No. ISO 7498-1984(E).

8. J. Postel, ed., IAB [Internet Activities Board] Official Protocol Standards, RFC 1140, May 1990.**

9. U.S. Department of Commerce, POSIX: Portable Operating System Interface for Computer Environments, Federal Information Processing Standards Publication 151-1, September 1989.

10. U.S. Department of Defense, Ada Programming Language, ANSI/MIL-STD-1815A, 22 January 1983.

11. Lester Sanders, Defense Electronics, June 1986, pp. 71-76.

12. U.S. Department of Defense, Trusted Computer System Evaluation Criteria, DoD Directive 5200.28-STD, December 1985.

13. Robert W. Shirey, "Defense Data Network Security Architecture", Computer Communication Review, Vol. 20, No. 2, April 1990, pp. 66-71.

14. David H. Crocker, Standard for the Format of ARPA Internet Text Messages, RFC 822, 13 August 1982.**

15. Jonathan B. Postel, Internet Protocol, RFC 791, September 1981.**

16. Jonathan B. Postel, Simple Mail Transfer Protocol, RFC821, August 1982.**

17. J. Linn, Privacy Enhancement for Internet Electronic Mail: Part I, RFC 1113, August 1989.**

18. Gary L. Tater and Edmund G. Kerut, "The Secure Data Network System", 10th National Computer Security Conference, September 1987, pp. 150-151.

19. William Stallings, Tutorial: Integrated Services Digital Networks (ISDN), IEEE Computer Society Press, Washington, D.C., 1988.

20. International Telephone and Telegraph Consultative Committee, Draft Recommendation X.400, Message Handling System and Service Overview, 1988.

21. -----, ----- X.500, The Directory - Overview of Concepts, Models, and Services, 1988

22. Ruth Nelson, "SDNS Services and Architecture", 10th National Computer Security Conference, Washington, D.C., September 1987, pp. 153-157.

23. Paul A. Lambert, "Architectural Model of the SDNS Key Management Protocol", 11th National Computer Security Conference, October 1988, pp. 126-128.

24. Phillip Gross and Richard Wilder, The Department of Defense Open Systems Interconnection (OSI) Implementation Strategy, MTR-87W00155, The MITRE Corporation, McLean, Va., May 1988.

THE AUTHOR

With a BS in Mathematics and an MS and PhD (1969) in Computer Science from the University of Wisconsin, Dr. Shirey left Madison for warmer weather, lower levels of ragweed pollen, and work as an assembler-language programmer for computer operating systems, a commission salesman for computer time-sharing systems, and a management consultant for government data-processing systems. At MITRE since 1977, he is now a Principal Scientist in the Security Technical Center of MITRE's Washington C^3I Division.

ACKNOWLEDGEMENTS

The author recognizes the contributions of the members of the DMS community to the TAIS, from which much of this paper was derived. The author also appreciates the helpful comments of Tom Clarke and Oma Elliott of DoD, Walt Kinzinger and Sam Schaen of MITRE, and the editor.