Department of Veterans Affairs
Washington, DC 20420

VA Directive 6103
Transmittal Sheet
March 23, 1998

VA ELECTRONIC MAIL SYSTEM

1. REASON FOR ISSUE: This directive establishes policy concerning the integration and implementation of an integrated Department-wide electronic mail (e-mail) system. The Telecommunications Strategic Planning Group (TSPG), which has representation from all organizations, voted unanimously on the need for a standard e-mail system and policy.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This directive defines the responsibilities for implementing a standard e-mail system. It contains a list of attributes that the e-mail software shall consist of, as well as references related to electronic messages.

3. RESPONSIBLE OFFICE: The VA's Information Resources Management (IRM) Policy and Standards Service (045A3), Office of the Deputy Assistant Secretary for IRM, is responsible for the material contained in this directive.

4. RELATED HANDBOOK: None.

5. RESCISSIONS: None.

CERTIFIED BY:

Nada D. Harris
Deputy Assistant Secretary for
Information Resources Management

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

D. Mark Catlett
Acting Assistant Secretary for Management

Distribution: RPC: 6006
FD

VA ELECTRONIC MAIL SYSTEM

1. PURPOSE. This directive establishes policy and responsibilities for integrating electronic mail (e-mail) systems throughout VA. It is the goal of VA to have an integrated Department-wide e-mail system that will allow any VA employee to communicate by e-mail with any other VA employee. In addition, the e-mail system should be designed in a manner that provides VA employees with the ability to communicate by electronic means when conducting business with VA beneficiaries, the public, and the private sector.

2. POLICY

a. It is the policy of the Department that all VA organizations adhere to government-wide and Departmental policies governing the creation, maintenance, security, and disposition of the e-mail system for information transmitted, processed, or stored.

b. The e-mail system must comply with the standard as specified in the effective version of Federal Information Processing Standard 146, "Profiles for Open Systems Internetworking Technologies (POSIT)." The National Institute of Standards and Technology (NIST) program, which provides for POSIT conformance testing and certification by commercial laboratories, shall be used in accordance with NIST guidelines. Also, NIST guidelines for approved interoperability testing and registration services shall be used**.**

c. VA will ensure that Information Technology (IT) and telecommunications policies and procedures apply to planning and use of the VA-owned e-mail systems as well as e-mail services provided by other government agencies or commercial sources to include FTS 2000 as it pertains to networking services (Reference VA Directive 6100, Telecommunications (Pending).Existing MP-6, PTI, Chapter 14 & 15).

d. The e-mail system, as an information system, shall comply with all applicable Automated Information System (AIS) security standards for information systems, including the Computer Security Act of 1987; OMB Circular A-130, Appendix III; VA Automated Information Security System Policy; and, when applicable, local AIS security policies.

e. VA will comply with the Departmental definitions and policies for records management that are contained in VA Directive 6300, Records and Information Management. Where Departmental policies for records management apply to electronic messaging information, VA Directive 6301, Electronic Mail Records, VA shall follow the policies and procedures for records retention and disposal, and will determine the office of record for each category of records.

f. VA e-mail system information may be subject to 5 U.S.C. 552a, Privacy Act of 1974, as amended. Responsible authorities shall review and implement VA Directive 6210, Automated Information Security System Directive.

g. The Department's POSIT name and address administration official shall insure that all e-mail systems are assigned POSIT names and addresses in accordance with Departmental procedures.

h. The Department's POSIT name and address administration official shall insure that all e-mail systems have a top-level folder called "VA", for department-wide use. There will also be a top-level folder for each major organization element for information specific to that organization.

i. E-mail will be used where it provides a cost-effective means for employees to conduct official business and improve delivery of service to veterans.

j. The administration and staff office components of the Department-wide e-mail system will be acquired, developed, and implemented in a coordinated and integrated manner that maximizes the ability of VA employees to send e-mail to and receive e-mail from VA employees, VA beneficiaries, the public, and the private sector.

3. RESPONSIBILITIES

a. **Secretary of Veterans Affairs.** The Secretary has designated the Department's Chief Information Officer (CIO) as the senior agency official responsible for the Department's IRM program.

b. **Chief Information Officer.** The CIO through the Deputy Assistant Secretary for Information Resources Management (DAS/IRM) will:

(1) review this policy on an annual basis to recommend any necessary revisions that will assist VA in migrating to a comprehensive e-mail solution that permits VA employees to send and receive e-mail when conducting business with other VA employees, beneficiaries, and the public and private sectors;

(2) ensure compliance with government-wide POSIT policies and standards;

(3) develop and administer POSIT Departmental policy and guidance;

(4) provide program coordination and liaison with the General Services Administration, other Federal agencies, and the FTS 2000 service provider;

(5) disseminate current POSIT standards and interoperability to staff offices;

(6) ensure that each major organization establishes a public folder using VA's standard naming convention and assign an individual to be responsible for administering the public folders;

(7) ensure that the e-mail system is implemented Department-wide;

(8) ensure that in-process/post implementation reviews are conducted periodically;

(9) ensure that the Department-wide e-mail standards are published and followed to provide the needed integrated capability;

(10) ensure that the e-mail system meets the Department's information security requirements; and,

(11) appoint a Department POSIT name and address administration official. The official shall ensure that all e-mail systems are assigned POSIT names and addresses in accordance with Departmental procedures.

c. **Administration Heads, Assistant Secretaries, and Other Key Officials** will ensure that:

(1) name and address coordination occurs between the Department FTS 2000 designated agency representative (DAR) and the Department name and address administration contact;

(2) Department e-mail system procedures are established to insure that:

(a) local systems are configured for efficient and cost-effective operations. POSIT X.400 systems may communicate in Administrative Management Domain (ADMD) to Private Management Domain (PRMD) and/ or PRMD-PRMD modes;

(b) the assignment of Originator/Recipient (O/R) names and POSIT addresses is coordinated with their designated name and address administration office; and,

(c) guidelines are established to ensure that reliability and quality service is maintained in e-mail systems.

(3) when a new e-mail system is being planned or when significant changes are being made to an existing system the appropriate Department Privacy Act officer is informed;

(4) an e-mail system is acquired and implemented Department-wide, which meets the users' requirements;

(5) a system liaison is appointed to serve as his/her organization's initial point of contact (POC) for troubleshooting, user orientation, training and support;

(6) users will receive training on a timely basis; and,

(7) users are required to change the temporary password that is originally issued to them the first time they log onto the VA e-mail system.

4. REFERENCES

a. Computer Security Act of 1987, PL 100-235, 101 Stat. 1724.

b. FIPS 146, Profiles for Open Systems Internetworking.

c. VA Directive 6100, Telecommunications (Pending).
(Existing MP-6, PTI, Chapter 14 & 15)

d. VA Directive 6300, Records and Information Management.

e. VA Directive 6210, Automated Information Systems Security.

f. VA Handbook 6301, Electronic Mail Records.

g. 36 CFR, section 1234, Electronic Records Management.

5. DEFINITIONS

a. **Electronic Mail.** A document created or received on an electronic mail system including brief notes, more formal or substantive narrative documents, and any attachments, such as word processing and other electronic documents, which may be transmitted with the message.

b. **Electronic Mail System.** Computer applications used to create, receive, and transmit messages and other documents. Excluded from this definition are file transfer utilities (software that transmits files between users but does not retain any transmission data), data systems used to collect and process data that have been organized into data files or data bases on either personal computers or mainframe computers, and word-processing documents not transmitted on an electronic mail system.

ATTRIBUTES FOR DEPARTMENT-WIDE E-MAIL SYSTEM

An electronic mail (e-mail) system is a computer application used to create, receive, and transmit text, audio, visual messages and other documents. The software package shall consist of the following attributes:

1. VA directory will be easy to maintain and contain customer demographic information for identification and selection of mail recipients by the letters in the recipients' last names;

2. message creation capability that provides word-processing features including word wrapping, full-screen editing, insertion, deletion;

3. direction of messages to all users, to single users, to dynamically defined groups of users, and to users on a designated distribution list. It must be possible to control user access or modification to this distribution list;

4. blind copy, courtesy copy, and automatic copy, which includes the distribution list author. The author copy should be stored in the sent box;

5. notification of users when they receive a message by audio and visual signal;

6. automatic date and time stamping;

7. notification of users if they have unread mail;

8. storage of deleted messages for later restoration;

9. forwarding of mail to other users or groups of users with name of originator and forwarder retained;

10. automatic identification of message originator, all authors of replies, date, time and subject to allow users to easily identify and select items for review or printing;

11. retrieval and deletion of mail;

12. delivery and read notification at senders option;

13. address mail via recipients' names rather than via directory;

14. directory search for names, using last name; first name;

15. reply to messages without creating a separate message and without having to enter a destination address (automatic default to the sender);

16. verification of distribution list before sending mail;

17. attachment of a word-processing document or any other file to an electronic mail message in the same or other VA platforms with retention of all formatting;

18. printing of text mail messages and saving in text form for subsequent conversion to word-processing format;

19. transmission and reception of messages with non-text enclosures (i.e., audio, visual);

20. creation of user-defined mailboxes;

21. access to private mailboxes by others as defined by the owner of the mailbox;

22. protection against loss of messages if a node malfunctions during transmission;

23. assignment of message importance levels and support for certification of message receipt;

24. a wide area network user capacity to allow full utilization by the VA customer base;

25. inspection of the list of recipients of a message, except for items sent to recipients as blind copy;

26. location of messages within a user's mailbox by sender, subject, or date;

27. support directory administrative functions that require registration (addition), modification or deletion of users to be completed only once within the electronic mail network;

28. encryption of sensitive data; and,

30. inter-agency, public, and private sector communications via the internet.