

ORDER

U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

1370.81A

5/13/02

SUBJ: ELECTRONIC MAIL

- 1. PURPOSE.** This order establishes agencywide policy on the use, operation, and management of the Federal Aviation Administration (FAA) administrative electronic mail (e-mail) system by FAA users (e.g., employees and contractors using FAA equipment). The administrative e-mail system is defined as the e-mail system that is used for general, non-classified, electronic business communication.
- 2. DISTRIBUTION.** This order is distributed to the Washington headquarters division level, regions, and centers; a limited distribution to all field offices and facilities; and to all information resource managers. A copy of this policy will be furnished to all new employees during employee orientation.
- 3. CANCELLATION.** Order 1370.81, Electronic Mail Policy, dated August 12, 1998, is canceled.
- 4. BACKGROUND.**

 - a.** In 1991, the FAA selected Lotus cc:Mail as the agency e-mail system. Use of the product grew over the years to include more personnel, but this growth was not standardized or centrally managed. Administration of e-mail was also decentralized, with post offices being established by lines of business (LOBs) as local area networks were implemented. The number of post offices grew from the initial 30 to 855, creating administrative and configuration management challenges.
 - b.** In October 2001, support of cc:Mail was discontinued by Lotus, requiring the agency to migrate to a new product. Implementation of the next generation (NexGen) messaging system to replace cc:Mail is currently underway. Implementation of a new e-mail system affords the agency the opportunity to address current e-mail architectural and administrative deficiencies and to introduce enterprise-wide efficiencies.
- 5. EXPLANATION OF CHANGES.** This revision:

 - a.** Establishes the agency policy on authorized use of the FAA e-mail system.
 - b.** Directs e-mail team administrators to comply with standard operating procedures.
 - c.** Designates the Information Technology Division (ASU-500) in the Office of Acquisitions (ASU) as the program office responsible for planning, budgeting, and operating the FAA e-mail system.
 - d.** Establishes the NexGen Program Team within the Integrated Product Team for Information Systems, ASU-510, to implement and manage the NexGen messaging system.
 - e.** Assigns responsibility for configuration management of the FAA e-mail system to the ASU-500 Configuration Control Board (CCB).

f. Designates the NexGen messaging system as the official e-mail system of the FAA and requires LOBs and staff offices (SOs) to obtain written approval from the Associate Administrator for Research and Acquisitions, ARA-1, Assistant Administrator for Information Services and Chief Information Officer, AIO-1, and Associate or Assistant Administrator for the requesting LOB or staff office prior to establishing an independent or parallel e-mail system.

g. Establishes criteria for handling sensitive information and remote access to the e-mail system.

6. DEFINITIONS. Appendix 1, Definitions, defines the terms used in this order.

7. RELATED LEGISLATION AND DIRECTIVES. Appendix 2, Related Legislation and Directives, contains legislation and directives that apply to e-mail systems.

8. SCOPE. This order applies to all offices, services, regions, centers, employees, contractors, support personnel, and all others who use or administer the FAA e-mail system.

9. POLICY. The FAA e-mail system shall be used to improve information dissemination and support business transactions within prescribed mandates, laws, and restrictions.

a. Use of the FAA E-Mail System. The FAA e-mail system shall be available only for authorized activities, as detailed in this paragraph.

1) Authorized Use. The FAA e-mail system shall be used:

(a) For valid work requirements (e.g., exchange of information that supports the FAA mission, goals, and objectives; and business-related communications with colleagues within the FAA, the public, other Government agencies, academia, industry, and international civil aviation authorities).

(b) For limited personal use (e.g., brief communications), provided such use does not:

- 1 Interfere directly or indirectly with FAA computer or networking services;
- 2 Burden FAA with additional incremental costs;
- 3 Interfere with an FAA user's employment or other obligations to the Government;
- 4 Reflect negatively on the FAA or its employees; or
- 5 Violate any Federal or FAA rules, regulations, or policies.

2) Unauthorized Use. Improper use of the FAA e-mail system includes:

(a) Using the FAA e-mail system for any purpose that violates the law or FAA rules, regulations, and policies;

(b) Concealing or misrepresenting user identity or affiliation in electronic messages;

(c) Accessing or altering source or destination addresses of e-mail;

(d) Intentionally propagating chain letters, broadcasting inappropriate or unsolicited messages (e.g., non-business matters) to lists or individuals, and comparable resource-intensive unofficial activity;

(e) Using the FAA e-mail system for any commercial purpose, for financial gain, or in support of outside individuals or entities;

- (f) Intentionally viewing, transmitting, collecting, or storing vulgar, abusive, discriminatory, obscene (including sexually explicit or pornographic materials), or harassing messages or material;
- (g) Attempting to libel, slander, or harass other users;
- (h) Posting to external newsgroups, bulletin boards, or other public forums, unless it is a business-related requirement, closely related to the employee's area of expertise, and appropriate office approvals have been obtained;
- (i) Engaging in matters directed toward any unauthorized fundraising, lobbying, or partisan political activities; and
- (j) Representing the agency in an official capacity when not authorized to do so.

b. Conduct on the FAA E-mail System by FAA Users. Standards of ethical conduct and appropriate behavior apply to the use of FAA computer networks, including the FAA e-mail system. All FAA users shall conduct activities on the FAA e-mail system with the same integrity as in face-to-face business transactions.

c. All information created, transmitted, received, obtained, accessed, or in any way captured electronically using the FAA e-mail system is the property of the U.S. Government.

d. The FAA e-mail system is a corporate resource that will be centrally monitored and funded by ASU-500 to improve system efficiency and reduce costs.

e. The NexGen messaging system is the official FAA e-mail system. No other e-mail systems will be established unless authorized by AIO-1.

f. A single message store will serve all local and remote users at any site where it is located.

g. Any system or architectural changes to the e-mail system must be approved by the ASU-500 CCB.

10. POLICY IMPLEMENTATION. This order establishes the principles by which the agency will manage the FAA e-mail system. There will be a nationally standardized implementation and administration, and a controlled configuration throughout the full life cycle. The NexGen Program Team will provide training for both users and administrators; e-mail servers and warranty service; software, including all upgrades; and a national helpdesk that operates 24 hours a day, 7 days a week. Because the program will operate across existing LOBs and SOs, the following framework is established within which the national program will operate:

a. An e-mail team will co-manage the message store at each site. The team will be composed of experts in e-mail administration from participating organizations.

b. Responsibility and accountability for coordinating the activities of the e-mail team, scheduling after-hours "on-call" support among the team members, and reporting team status to the NexGen Program Team, rests with the e-mail team leads. Team leads shall be staffed by the Office of the Associate Administrator for Research and Acquisitions at Washington headquarters and the William J. Hughes Technical Center (ACT), and the Office of the Assistant Administrator for Region and Center Operations (ARC) at the regional offices and Mike Monroney Aeronautical Center (MMAC). Team leads for all teams have the primary responsibility for ensuring that database-wide (message store) maintenance requirements are accomplished.

c. All team members will have full access rights to the message store and will perform database-wide activities when required and/or scheduled.

d. The NexGen Program Team will provide technical guidance and direction to the e-mail teams.

e. A single Standard Operating Procedure (SOP) for the administration and management of the FAA e-mail system will be implemented at all message store locations. The e-mail system SOP shall be published and maintained by the NexGen Program Team.

f. Based on demonstrated performance (as determined by the LOBs), full e-mail responsibility at the regional offices and the MMAC is anticipated to transition to ARC. As stated in paragraph 10.b., Washington headquarters and ACT will be managed by ARA.

11. RESPONSIBILITIES.

a. E-mail users shall:

1) Utilize e-mail only in support of their official duties and responsibilities, except as specified in this order for limited incidental use.

2) Identify and preserve e-mail messages that are official records, consistent with paragraph 12 of this order.

3) Follow all rules of information security and privacy including those detailed in paragraphs 13 and 14 of this order.

b. FAA LOBs and SOs shall:

1) Determine who in their LOB/SO will have access to the FAA e-mail system and ensure that all users have a copy of, and are familiar with, this order.

2) Notify their e-mail administrator of new users who require an e-mail account and of users who leave the organization and whose account should be removed.

3) Maintain client configurations locally on the desktops of their users, unless arrangements for maintenance are made with a servicing organization through a Service Level Agreement.

4) Provide an e-mail administrator to the team if participating in the administration and management of the message store, and ensure that he/she receives all necessary training provided by the NexGen Program Team.

c. E-mail teams shall:

1) Manage the e-mail message store(s) and user accounts assigned to them.

2) Follow e-mail administrative procedures as specified by the e-mail system SOP.

3) Maintain system files, connectivity, discussion databases (formerly called bulletin boards), mailing lists, and automated directory exchanges.

4) Relay broadcast messages in accordance with the standards and guidelines established by the ASU-500 CCB to ensure that all FAA employees have access to the information.

5) Support all users in their message store.

6) Supply technical expertise to the ASU-500 CCB, as requested.

7) Participate in after-hours support coverage, as a backup to the national helpdesk.

8) Provide backup to other team members as approved and coordinated.

9) Provide information systems security for the message store under their administration in accordance with existing rules and regulations.

d. E-mail team leads shall, in addition to the above responsibilities:

- 1) Provide administration for the user accounts of those organizations, both remote and local, that are not participating in the e-mail team.
- 2) Coordinate the scheduling of database-wide maintenance activities and ensure their successful completion.
- 3) Coordinate the scheduling of after-hours support coverage in conjunction with the LOB manager.
- 4) Serve as primary point of contact between the NexGen Program Team and the e-mail team.

e. The NexGen Program Team in the Integrated Product Team for Information Systems, ASU-510, shall:

- 1) Provide program management consistent with the requirements of this order including planning, budgeting, and operation.
- 2) Provide a central, top-level mail store/hub, a master e-mail directory, and connectivity to Internet e-mail services.
- 3) Supply hardware and/or software upgrades, electronic documentation, and helpdesk support.
- 4) Provide all required training for operation and maintenance of the e-mail system.
- 5) Provide information systems security for the FAA e-mail system in accordance with existing rules and regulations.
- 6) Implement a filter at the system level based on the Sensitive Security Information (SSI) Access List developed by AIO and the LOB/SOs to prevent SSI from being inadvertently sent to the wrong recipient.

f. The Assistant Administrator for Information Services and Chief Information Officer, AIO-1, shall:

- 1) Develop policy and requirements for the creation, performance, and oversight of the FAA e-mail system.
- 2) Review and approve or disapprove requests for establishment of parallel e-mail systems.
- 3) In conjunction with the LOB/SOs, develop and provide to ASU-500 the SSI Access List to be used as the system level filter to prevent SSI from being inadvertently sent to the wrong recipient.

g. The Director, Office of Personnel, AHP-1, shall ensure a copy of this policy is furnished to all new employees during employee orientation.

h. The ASU-500 CCB shall manage the FAA e-mail system as a configuration item under its charter. The ASU-500 CCB shall:

- 1) Approve and implement the CCB operating procedures and configuration management change request process documents and any changes to these documents for the FAA e-mail system.

- 2) Develop procedures and guidelines for the creation, performance, and oversight of the FAA e-mail system.
- 3) Establish baselines for systems/services and control subsequent changes to the FAA e-mail system.
- 4) Ensure adherence to configuration control procedures in processing changes to the FAA e-mail system baseline under this CCB's control.
- 5) Ensure that the changes to baselined documents for the FAA e-mail system are presented to this CCB for approval.
- 6) Review proposed changes to the FAA e-mail system baseline for potential impacts.
- 7) Ensure that the proposed changes to the FAA e-mail system are coordinated with interface/impacted organizations.
- 8) Adjudicate proposed changes to the FAA e-mail system presented to this CCB, ensuring an accurate review and thorough evaluation.
- 9) Issue ASU-500 CCB Action Forms documenting actions taken by the CCB regarding each change request for the FAA e-mail system, including assigning action items as necessary.
- 10) Ensure action items for the FAA e-mail system are completed as directed.
- 11) Ensure, through Configuration Status Accounting, that all approved changes to the FAA e-mail system are tracked, documented, and completed.

12. RECORDS MANAGEMENT.

- a. The FAA e-mail system is not an approved official records system.
- b. All government employees and contractors are required by law to make and preserve records containing evidence of the organization, functions, policies, decisions, procedures, and essential transactions of the agency. These records must be properly maintained and preserved as prescribed in Order 1350.14, Records Management, as follows:
 - 1) The sender of an FAA created e-mail is responsible for preserving the record.
 - 2) The office responding to an external e-mail is responsible for preserving the incoming e-mail as a agency record.
 - 3) All other recipients' copies of the e-mail are not records and may be destroyed when no longer needed.
- c. Any electronic materials that are determined to be records shall be disposed of in compliance with the General Records Schedules as published by the National Archives and Records Administration or FAA specific archivist-approved records schedule, such as Order 1350.15, Records Organization, Transfer, and Destruction Standards.
- d. Users may purge or delete e-mail and attachments that are official FAA records after printing and storing or properly electronically storing in an approved official records system.

13. SECURITY.

a. Classified Information. The FAA e-mail system shall not be used for the creation, storage, processing, or transmission of any classified information.

b. Privacy/Confidentiality. The contents of U.S. Government-owned and/or funded electronic information systems, including e-mail, are the property of the U.S. Government and may be subject to audit and inspection. No FAA user should have the expectation of personal privacy or ownership using any FAA electronic information or communication equipment.

c. Unauthorized Access. Unauthorized access includes, but is not limited to, access beyond an individual's authorization limits and accessing the contents of another individual's (or group's) e-mail. Order 1370.82, Information Systems Security Program, requires that information be properly protected from unauthorized access.

d. Sensitive Information. Sensitive information is information meeting specific standards that require additional protection against unauthorized disclosure (i.e., the Trade Secrets Act or 14 CFR, Part 191). When using the FAA e-mail system to forward sensitive information, the following procedures shall be followed:

- 1) Protective markings and handling instructions shall be inserted in the header and footer of the document to identify it as sensitive information and to advise the recipient of its sensitive nature.
- 2) In the event that sensitive information is being forwarded outside the FAA e-mail system, the strongest protection provided by the FAA e-mail system should be applied (e.g., encryption or password protection).
- 3) Sensitive-but-unclassified e-mail, such as those received from the Defense Messaging System, should be considered sensitive information and handled accordingly.

e. Sensitive Security Information (SSI). SSI is information obtained or developed in carrying out certain security or research and development activities (14 CFR part 191). When using the FAA e-mail system to forward SSI, the following procedures shall be followed:

- 1) Protective markings and handling instructions shall be inserted in the header and footer of the document to identify it as SSI and advise the recipient of its SSI nature.
- 2) The strongest available protection provided by the FAA e-mail system should be applied to SSI (e.g., encryption or password protection).
- 3) Electronic filters will be implemented at the systems level to prevent e-mailing SSI to the wrong recipient.

f. Remote Access. FAA e-mail users will use only those remote access methods approved by the CCB as part of the system/services baseline.

14. PRIVACY ACT. The use of e-mail to transfer information covered under the Privacy Act should not be done, as this leaves that information extremely vulnerable to inadvertent or improper disclosure. The transfer of Privacy Act information in the body of an e-mail or the attachment of a Privacy Act record to an e-mail allows that information to be forwarded to other, possibly unauthorized, personnel or to be printed and left visible for unauthorized personnel to see. Refer to Order 1280.1, Protecting Privacy of Information About Individuals, for further information on the Privacy Act.

15. FREEDOM OF INFORMATION ACT (FOIA). E-mail messages and attachments are subject to FOIA requests. Under the FOIA, users and system administrators are obligated to conduct a reasonable search of all FAA information and records, including electronic data, that could be responsive to the request. Searches of these electronic files are pursued to the same extent that such searches would be pursued in general hard copy files. Refer to Order 1270.1, Freedom of Information Act Program, for further information on FOIA.

16. REQUESTS FOR INFORMATION. Information requests concerning this e-mail policy may be addressed to the Office of Information Services, Information Management Division (AIO-300).

A handwritten signature in cursive script, appearing to read "Jane F. Garvey".

Jane F. Garvey
Administrator

APPENDIX 1: DEFINITIONS

1. **After-hours support.** Because of the importance of e-mail to the efficiency of the FAA, there is a requirement for user support beyond the normal work day. The national helpdesk provided by the NexGen Program Team will be the primary after-hours support. As backup to the national helpdesk, each e-mail team will participate in after-hours coverage consistent with the needs of the LOBs being served by that team.
2. **cc:Mail.** The agency e-mail application replaced by the NexGen e-mail system.
3. **Configuration Control Board (CCB).** The board given authority to manage the e-mail system configuration.
4. **E-Mail Teams.** These consist of individuals that have been identified by their LOB or staff office CIO, and trained by NexGen to manage the Lotus Domino servers located in each of the 12 FAA regional offices. In their current form, these are the NexGen Regional Messaging Administration Teams, however, this organizational structure could be modified at some future date if all parties agreed to a new structure.
5. **FAA users.** Individuals authorized to use FAA electronic information systems, including the FAA e-mail system, as part of their assigned duties. This includes FAA employees and support contractors.
6. **Message Store.** A message store is defined as the messaging server location where a users' messages, folders, personal address books, and personal mailing lists are physically stored. This definition will be extended to include the physical storage location of calendaring information, document storage, and workflow components as these functions are added.
7. **NexGen.** The next generation messaging system FAA e-mail application.
8. **Standard Operating Procedures (SOPs).** E-mail system administrative procedures approved and distributed by the NexGen Program Team.

APPENDIX 2: RELATED LEGISLATION AND DIRECTIVES

1. 14 Code of Federal Regulations (CFR), Part 191.
2. Computer Fraud and Abuse Act of 1986.
3. Computer Security Act of 1987.
4. Departmental Information Resource Management Manual (DIRMM) DOT H 1350.2, Electronic Mail.
5. Electronic Communications Privacy Act of 1986.
6. Executive Orders 12674 and 12731, Principles of Ethical Conduct of Government Officers and Employees; 5 CFR Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch; and 5 CFR Chapter L.
7. Federal Records Act (44 USC Chapters 29, 31, 33, and 35).
8. Freedom of Information Act.
9. Office of Management and Budget Circular A-130, Management of Federal Information Resources, dated February 20, 1996.
10. Order 1270.1, Freedom of Information Act Program, dated June 13, 2000.
11. Order 1280.1A, Protecting Privacy of Information About Individuals, dated October 7, 1994.
12. Order 1370.79A, Internet Use Policy, dated October 12, 1999.
13. Order 1370.82, Information Systems Security Program, dated June 9, 2000.
14. Order 1600.2D, Safeguarding Controls and Procedures for Classified National Security Information and Sensitive Unclassified Information.
15. Paperwork Reduction Act of 1995.
16. Policy Memorandum ACP-300-99-001, Safeguarding and Control of Sensitive Security Information, dated November 30, 1998.
17. Privacy Act of 1974.
18. Trade Secrets Act.