''major rule'' as defined by 5 U.S.C. 804(2).

C. Petitions for Judicial Review

Under section 307(b)(1) of the Clean Air Act, petitions for judicial review of this action to extend the deadline for incorporation of on-board diagnostics checks to the Pennsylvania I/M program by one year must be filed in the United States Court of Appeals for the appropriate circuit by August 5, 2002. Filing a petition for reconsideration by the Administrator of this final rule does not affect the finality of this rule for the purposes of judicial review nor does it extend the time within which a petition for judicial review may be filed, and shall not postpone the effectiveness of such rule or action. This action may not be challenged later in proceedings to enforce its requirements. (See section 307(b)(2).)

List of Subjects in 40 CFR Part 52

Environmental protection, Air pollution control, Carbon monoxide, Hydrocarbons, Nitrogen dioxide, Ozone.

Dated: May 29,2002.

William C. Early,

Acting Regional Administrator, Region III.

40 CFR part 52 is amended as follows:

PART 52—[AMENDED]

1. The authority citation for part 52 continues to read as follows:

Authority: 42 U.S.C. 7401 *et seq.*

Subpart NN—Pennsylvania

2. Section 52.2022 is amended by adding paragraph (f) to read as follows:

§ 52.2022 Extensions

* * * * *

(f) The Administrator hereby extends by 12 months the deadline by which Pennsylvania must incorporate mandatory testing of second generation on-board diagnostics (OBD-II) equipped motor vehicles as part of its inspection and maintenance (I/M) program. As a result of this deadline extension, Pennsylvania must now incorporate mandatory OBD-II checks (for 1996-and-newer OBD-II-equipped vehicles) as an element of the Commonwealth's I/M program in all enhanced I/M program areas by January 1, 2003.

[FR Doc. 02–14035 Filed 6–5–02; 8:45 am]

BILLING CODE 6560–50–P

GENERAL SERVICES ADMINISTRATION

41 CFR Parts 101–9 and 102–192

[FPMR Amendment A–58]

RIN 3090–AH13

Mail Management

AGENCY: Office of Governmentwide Policy, GSA.

ACTION: Interim rule.

SUMMARY: The anthrax crisis has made the health and security of Federal employees the primary concerns of the General Services Administration's (GSA's) mail communications policy program. GSA published a proposed rule in the **Federal Register** on May 29, 2001 (66 FR 29067) to solicit opinions from the mail community on changes to the mail regulation. GSA is publishing this interim rule now because it is critical that we provide updated mail security requirements and guidance as quickly as possible.

This is an interim rule because we recognize that the security and financial requirements in this rule will continue to evolve. Before formulation of the final rule, we will solicit agencies for comment. We are allowing time for agencies to gain experience with this interim rule prior to obtaining input for the final rule.

DATES: This interim rule is effective June 6, 2002.

ADDRESSESS: Send written comments to: Rodney Lantier, Regulatory Secretariat, Acquisition Policy Division (MVP), General Services Administration, 1800 F Street, NW., Washington, DC 20405. Send comments by e-mail to: *RIN.3090-AH13@gsa.gov.*

FOR FURTHER INFORMATION CONTACT: Henry Maury, Mail Communications Policy Division (MTM) or *henry.maury@gsa.gov.*

SUPPLEMENTARY INFORMATION:

A. Background

The purposes of this interim rule are to update and clarify FPMR part 101–9, Federal Mail Management, and move it into the Federal Management Regulation (FMR). This interim rule is written in a plain language, question and answer format. This style uses the active voice, shorter sentences, and pronouns. A question and its answer combine to establish a rule; that is, Federal agencies and Federal employees must follow the language contained in both the question and its answer.

Section 2 of Public Law 94–575, the Federal Records Management Amendments of 1976, as amended, directs the Administrator of General Services to provide guidance and assistance to Federal agencies on records management, including the processing of mail by Federal agencies, and this interim rule implements that direction. In doing so, this interim rule establishes four requirements for all agencies and four additional requirements for agencies that mail over $1 million annually. These requirements are described in sections 102–192.50 and 102–192.55 respectively.

Agency Comments on the Proposed Rule

In response to the proposed rule, we received comments from nineteen agencies, two boards and one from the private sector. All comments were considered in the formulation of this interim rule.

Several comments concerned the proper definition of ''user level''. The concept here is that Federal mailers, or users, will better manage their mailing expenses if they are charged for the actual cost of their mailings. The definition of ''user level'' was deliberately vague to allow agencies to define users in a way that best fit their organizations. For instance, an agency could define ''user'' as an organizational entity, program, or location. To make the concept clearer, we have changed the term to ''program level''.

Many respondents were also unclear how we defined ''system'' in the proposed regulation. We have added a definition in section 102–192.35 to explain the term.

To reduce the confusion over agency requirements, we have reorganized the interim rule to separate required actions from recommended actions.

The most frequent comment was that providing GSA with volumetric and cost data from users at all levels within the agency would be prohibitively expensive, would adversely impact mail delivery, and would not provide a benefit to the agencies or GSA. This interim rule alters the requirement by allowing agencies to gather the needed data by any method they deem appropriate. When more agencies have availed themselves of automated tools for gathering data on mail operations, this requirement will be revisited.

The proposed regulation required that agencies' financial accountability systems capture costs associated with mailing. So that we may address agencies' security concerns quickly, we are temporarily foregoing the financial accountability component of the proposed regulation. We plan to implement this requirement when

mailing and financial systems can more easily track costs. We will continue to work with the agencies' mail management plans and promote best practices towards this goal.

Many comments were received about the Official Mail Accounting System (OMAS)—see definition in section 102–192.35. In most agencies, OMAS does not account for mail below the Chief Financial Officer level and its use creates no incentive to save money on mail; the people who decide whether something should be mailed, what shape it should take, what postage should be applied, and how many copies should go out, are not the people who pay for the postage. Most Federal mailers, therefore, have little incentive to limit mailing costs.

The General Services Administration has discussed this situation with Federal financial experts, mail industry consultants, the Office of Management and Budget, and many Federal mail managers. Every private-sector expert that GSA has reached agrees that giving the program managers information about, and responsibility for, the money they spend on mail is critical to improved management and cost control. We have also studied the experience of the five Federal agencies (most notably the Department of Defense) that have converted all or part of their postage to commercial payment processes. On the basis of this discussion and consideration, the General Services Administration has decided to direct the Federal agencies that fall within its authority to stop using OMAS to account for postage and to pay for postage using commercial payment processes. The effective date for this direction is October 1, 2003.

When Federal line managers pay for postage the same way that private sector organizations do, and account for postage costs through their standard accounting and budget processes, they are able to:

Track postage costs in real time;

Measure performance;

Identify opportunities to save money before they spend it;

Identify instances of potential fraud;

Streamline operations and improve productivity;

Eliminate the extra administrative burden of a cumbersome system; and

Increase their ability to react quickly to problems.

We recognize that the transition to commercial payment for postage will be more complicated for some agencies than for others, but we have determined that it will benefit all Federal agencies and the taxpayers in the long run. We estimate savings resulting from Federal agencies' withdrawal from OMAS will be approximately $70 million annually across the government.

B. Executive Order 12866

GSA has determined that this interim rule is not a significant rule for the purposes of Executive Order 12866 of September 30, 1993.

C. Regulatory Flexibility Act

This interim rule is not expected to have a significant economic impact on a substantial number of small entities within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601, *et seq.*

D. Paperwork Reduction Act

The Paperwork Reduction Act does not apply because this interim rule does not impose recordkeeping or information collection requirements, or the collection of information from offerors, contractors, or members of the public which require the approval of the Office of Management and Budget (OMB) under 44 U.S.C. 3501, *et seq.*

E. Small Business Regulatory Enforcement Fairness Act

This interim rule is exempt from Congressional review prescribed under 5 U.S.C. 801 since it relates solely to agency management and personnel.

List of Subjects

41 CFR Part 101–9

Government property management.

41 CFR Part 102–192

Government contracts, Intergovernmental relations, Reporting and recordkeeping requirements, Security measurements.

For the reasons set forth in the preamble, 41 CFR chapters 101 and 102 are amended as follows:

CHAPTER 101—[AMENDED]

1. Part 101–9 is revised to read as follows:

PART 101–9—FEDERAL MAIL MANAGEMENT

Authority: Sec. 2, Pub. L. 94–575, as amended, 44 U.S.C. 2904; 40 U.S.C. 486(c); Sec. 205(c), 63 Stat. 390.

§ 101–9.000 Cross-reference to the Federal Management Regulation (FMR) (41 CFR chapter 102, parts 102–1 through 102–220).

For Federal mail management information previously contained in this part, see FMR part 192 (41 CFR part 102–192).

CHAPTER 102—[AMENDED]

2. Part 102–192 is added to subchapter G to read as follows:

PART 102–192—MAIL MANAGEMENT

Subpart A—General Provisions

Subpart B—General Requirements

Subpart C—Reporting Requirements

Subpart D—Security Provisions

Subpart E—Recommended Actions

Subpart F—Agency Mail Manager Responsibilities

Subpart G—Facility Mail Manager Responsibilities

Authority: Sec. 2, Pub. L. 94–575, as amended, 44 U.S.C. 2904; 40 U.S.C. 486(c); Sec. 205(c), 63 Stat. 390.

Subpart A—General Provisions

§ 102–192.5 What does this part cover?

This part prescribes policy and requirements for the efficient, effective, economical, and secure management of incoming, internal, and outgoing mail in Federal agencies.

§ 102–192.10 What authority governs this part?

This part is governed by Section 2 of Public Law 94–575, the Federal Records Management Amendments of 1976 (44 U.S.C. 2901–2904), as amended, which requires the Administrator of General Services to provide guidance and assistance to Federal agencies on records management and defines the processing of mail by Federal agencies as a records management activity.

§ 102–192.15 How are ''I'', ''you'', ''me'', ''we'', and ''us'' used in this part?

In this part, ''I'', ''me'', and ''you'' (in its singular sense) refer to agency mail managers and/or facility mail managers; the context makes it clear which usage is intended in each case. ''We'', ''us'', and ''you'' (in its plural sense) refer to your Federal agency.

§ 102–192.20 How are ''must'' and ''should'' used in this part?

In this part:

(a) ''Must'' identifies steps that Federal agencies are required to take; and

(b) ''Should'' identifies steps that GSA recommends.

§ 102–192.25 Does this part apply to me?

Yes, this part applies to you if you work in a Federal agency, as defined in § 102–192.35.

§ 102–192.30 What types of mail does this part apply to?

This part applies to all materials that might pass through a Federal mail processing center, including:

(a) All internal, incoming, and outgoing materials such as envelopes, bulk mail, expedited mail, individual packages up to 70 pounds, publications, and postal cards, regardless of whether or not they currently pass through a particular mail center;

(b) Similar materials carried by agency personnel, contractors, the United States Postal Service (USPS), and all other carriers of such items; and

(c) Electronic mail only if it is printed out and mailed as described in paragraphs (a) and (b) of this section; however, this part encourages agencies to maximize use of electronic mail in lieu of printed media, so long as it is cost-effective.

§ 102–192.35 What definitions apply to this part?

The following definitions apply to this part:

Agency mail manager means the person who manages the overall mail communications program of a Federal agency. The *agency mail manager* also represents the agency in its relations with mail service providers, other agency mail managers, and the GSA Office of Governmentwide Policy.

Class of mail means the 5 categories of domestic mail as defined by the United States Postal Service (USPS) in the Domestic Mail Manual, (C100 through C600.1.z). These are:

(1) Express Mail and Priority Mail.

(2) First Class.

(3) Standard Mail (e.g., bulk marketing mail).

(4) Package Services.

(5) Periodicals.

Commingling means the merging of outgoing mail from one facility or agency with outgoing mail from at least one other source.

Expedited mail is a generic term that means mail designated for delivery more quickly than the USPS's normal delivery times (which vary by class of mail). Examples of *expedited mail* include USPS Express Mail and overnight and two-day delivery by other service providers.

Facility mail manager means the person responsible for mail in a specific Federal facility. There may be many *facility mail managers* within a Federal agency. *See* subpart G of this part for additional information about facility mail managers.

Federal agency (or agency) means:

(1) Any executive department as defined in 5 U.S.C. 101;

(2) Any wholly owned Government corporation as defined in 31 U.S.C. 9101;

(3) Any independent establishment in the executive branch as defined in 5 U.S.C. 104; and

(4) Any establishment in the legislative branch, except the Senate, the House of Representatives, the Architect of the Capitol, and all activities under the direction of the Architect of the Capitol (44 U.S.C. 2901(14)).

Federal facility (or facility) means any office building, installation, base, etc., where Federal agency employees work; this includes any facility where the Federal government pays postage expenses even though few Federal employees are involved in processing the mail.

Incoming mail means any mail that comes into the agency delivered by any service provider, such as the USPS, UPS, FedEx, or DHL.

Internal mail means mail generated within a Federal facility that is delivered within that facility or to a nearby facility of the same agency, so long as it is delivered by agency personnel or a dedicated agency contractor (i.e., not a service provider).

Large agency means a Federal agency whose total annual mail payments to all service providers exceeds $1 million. See appendix A to this part for a current list of the large agencies.

Mail means the types of mail described in § 102–192.30.

Mail costs means allocations and expenses for postage and all other *mail* costs (*e.g.,* payments to service providers, mail center personnel costs, mail center overhead, etc.).

Mail piece design means laying out and printing items to be mailed such that they can be processed efficiently and effectively by automated mail-processing equipment.

Mail system means all of the components of your mail operation including your methods for capturing data on your mail users, their volumes, and costs. The *mail system* includes the financial and accounting systems. It can be automated, manual or both.

Official Mail Accounting System (OMAS) is the Postal Service's government-unique system used to track postage used by most Federal agencies. *OMAS* is used in conjunction with each agency's online payment and accounting system (OPAC) account at the Treasury.

Outgoing mail means mail generated within a Federal facility that is going outside that facility and is delivered by a service provider.

Postage means money due or paid to any service provider.

Presort means a mail preparation used to receive a discounted mailing rate by sorting mail according to USPS standards.

Program Level means a subsidiary part of a Federal agency that generates a significant quantity of outgoing mail. It could apply to an agency organizational entity, program, or project. (See subpart H of this part for additional information.)

Service provider means any agency or company that delivers mail. Some examples of service providers are USPS, UPS, FedEx, DHL, courier services, the Military Postal Service Agency, the State Department of Diplomatic Pouch and Mail Division and other Federal agencies providing mail services.

Special services means those mail services that require extra payment over basic postage; e.g., certified mail, business reply mail, registered mail, insurance, merchandise return service, certificates of mailing, return receipts, and delivery confirmation.

Unauthorized use of agency postage means the use of penalty or commercial mail stamps, meter impressions, or other postage indicia for personal or unofficial use.

Worksharing means cost-effective ways of processing outgoing mail that qualify for reduced postage rates; examples include presorting, bar coding, consolidating, and commingling.

§ 102–192.40 Where can I get more information about the classes of mail?

Details about mail classes can be found in the Domestic Mail Manual (DMM). The DMM is available from New Orders, Superintendent of Documents, U.S. Government Printing Office, P.O. Box 371954, Pittsburgh, PA 15250–7954, *http://pe.usps.gov/.*

§ 102–192.45 How do we request a deviation from these requirements, and who can approve it?

See §§ 102–2.60 through 102–2.110 of this chapter to request a deviation from the requirements of this part.

Subpart B—General Requirements

§ 102–192.50 What must all agencies do to manage their mail effectively and efficiently?

All agencies are required to:

(a) Have written security plans for mail operations at the agency level and in any facility where one or more full time personnel processes mail.

(b) Ensure that mail costs are identified at the program level within the agency; each agency will have to determine the appropriate level for this requirement because the level at which it is cost-beneficial differs widely. Program level costs can be identified from tracking mailing expenses by program areas, cost estimates, financial reports, reconciled Postal Service records, and reconciled vendor data.

(c) Beginning October 1, 2003, all payments to the United States Postal Service must be made using commercial payment processes, not OMAS.

(d) Have performance measures for mail operations at the agency level and in all subordinate locations that spend more than $250,000 per year on postage; it is up to each agency to select the actual performance measures used.

§ 192.55 What are the additional requirements for large agencies?

All agencies that spend more than $1 million per year on postage are additionally required to develop and maintain an annual mail management and security plan. The plan must:

(a) State total amounts paid to all service providers;

(b) Verify that facility security plans have been reviewed at the agency level. A copy of at least one large facility plan must be attached;

(c) Identify performance measures in use at the agency level;

(d) Identify the agency mail manager; and

(e) Describe the agency's plans to improve the economy and efficiency of mail operations.

Subpart C—Reporting Requirements

§ 102–192.60 What must we report to GSA about our mail operations?

If you meet the definition of a large agency (see § 102–192.35), you must report to GSA annually either your mail management and security plan, revised section(s) of that plan, or a statement verifying that your plan has been reviewed and that there are no changes to it. The annual report must state that all facility security plans have been reviewed by a competent authority within the past year.

§ 102–192.65 When must we submit reports to GSA about our mail?

If you meet the requirement in § 102–192.35, the first annual agency mail management and security plan to GSA covering Fiscal Year 2001 is due September 4, 2002. Thereafter, fiscal year reports will be due annually on March 30. You must promptly report the name of the agency mail manager whenever it changes. GSA maintains an updated list of Federal agency mail managers at *http://www.gsa.gov/mailpolicy.*

§ 102–192.70 What format should we use when reporting mail data to GSA?

GSA will provide the format and reporting process for submitting the agency's annual mail management and security plan. These will be developed in collaboration with the Interagency Mail Policy Council. The final reporting format will be posted on the Mail Policy Communications home page at *http://www.gsa.gov/mailpolicy.*

§ 102–192.75 Where do we send our mail management reports and security plan verifications?

Submit hardcopy mail reports to: General Services Administration, Office of Governmentwide Policy, Mail Communications Policy Division (MTM), 1800 F Street, NW., STE 1221, Washington, DC 20405–0002. Electronic submissions are encouraged. Submit electronic reports to: *federal.mail@gsa.gov.*

§ 102–192.80 Why does GSA require these mail reports?

GSA requires these annual agency mail management and security plans to:

(a) Ensure that the large Federal mail programs have the tools and procedures in place to manage their operations efficiently and effectively;

(b) Ensure that appropriate security measures are in place; and

(c) Allow GSA to fulfill its responsibilities under the Federal Records Act, especially with regards to sharing best practices, training, standards, and guidelines.

Subpart D—Security Provisions

§ 102–192.85 Must I have a mail security plan?

Every Federal agency and agency location where an agency has one or more full time personnel processing mail must implement a written mail security plan. The size and scope of the security plan should be commensurate with the size and responsibilities of each agency or location. The security plan should be updated whenever circumstances warrant. As a minimum, it should be reviewed annually.

§ 102–192.90 What must I include in the mail security plan?

Your security plan must include polices and procedures for safe and secure operations consistent with your agency's core mission. It must also include:

(a) Procedures for handling all incoming mail, regardless of service provider;

(b) Plans for security training for mail center personnel;

(c) Procedures for ensuring compliance with the standards

established by the Interagency Security Committee that was established in accordance with Executive Order 12977, dated October 19, 1995 (3 CFR, 1995 Comp., p. 413). These standards can be found at *http://www.oca.gsa.gov;*

(d) A list of all large facilities, their points of contact and telephone numbers; and

(e) Plans for annual reviews of the agency's security plan and facility-level security plans.

§ 102–192.95 What else should I include in the mail security plan?

Additionally, your plan should ensure that:

(a) Facility mail managers participate in their building security committees, wherever such committees exist;

(b) Mail is transported in a safe manner;

(c) X-raying of mail occurs where appropriate; and

(d) The standards outlined in appendix B to this part are implemented.

Subpart E—Recommended Actions

§ 102–192.100 What financial system features does GSA recommend for finance systems to keep track of mail costs?

Agencies should develop or use a financial accountability system that separately tracks all mail costs to the program area or below. The system should:

(a) Show allocations and expenses for postage and all other mail costs (*e.g.,* payments to service providers, mail center personnel costs, mail center overhead, *etc.*) separate from all other administrative expenses;

(b) Assign control of funds for postage to the same person who has overall authority to control mail decisions for the program area;

(c) Allow mail centers to establish systems to charge their customers for postage; and

(d) Identify and charge mail costs that are part of printing contracts to the program level.

§ 102–192.105 What performance goals and measures should we use?

Section 102–192.50 requires all large agencies to have performance measures for mail operations at the agency level and in all subordinate locations that spend more than $250,000 per year on postage. All other agencies are also encouraged to identify performance goals and measures for incoming and outgoing mail operations. Your performance measurement efforts should be focused on the large facilities that generate most of your mail. The range of measures will depend on the size of your agency or facility, your mission, and the life cycle cost of data collection. GSA will provide suggested performance measures through its mail policy website.

§ 102–192.110 What should your agency-wide mail management plan include?

Your agency-wide mail management plan should address:

(a) The ways in which mail management supports your agency's mission;

(b) Information about your agency's primary facilities;

(c) Opportunities for reducing costs and/or enhancing your agency's ability to perform its mission through better mail management;

(d) How you choose the lowest cost and/or best value service provider(s) for outgoing mail, while ensuring that the Private Express Statutes and all USPS regulations are followed;

(e) Opportunities for centralized mail processing, worksharing, consolidation, and commingling to obtain postage savings;

(f) How and to what extent you will move toward ensuring that the person who controls mail decisions is the same person who controls the funds for postage;

(g) How and to what extent you will move toward ensuring that your financial systems show allocations and expenses for postage and all other mail costs separately from all other administrative expenses; and

(h) How you are developing specific performance goals, maintaining performance data systems and relating mail management goals to your agency's mission-related goals.

§ 102–192.115 What less costly alternatives to expedited mail and couriers should your agency-wide mail management plan address?

Your plan should address the following alternatives to expedited mail and couriers:

(a) First Class and Priority Mail from the USPS;

(b) Package delivery services from other service providers; and

(c) Electronic transmission via e-mail, facsimile transmission, electronic commerce, the Internet, etc.

Subpart F—Agency Mail Manager Responsibilities

§ 102–192.120 What is the appropriate managerial level for an agency mail manager?

The agency mail manager should be at a managerial level that enables him or her to fulfill the requirements of §§ 102–192.50 through 102–192.65 and § 102–192.125.

§ 102–192.125 What are my general responsibilities as an agency mail manager?

In addition to carrying out the responsibilities in § 192.50, an agency mail manager should:

(a) Establish written policies and procedures to provide timely and cost effective dispatch and delivery of mail;

(b) Ensure agency-wide awareness and compliance with standards and operational procedures established by all service providers used by the agency;

(c) Monitor the agency's mailings and other mail management activities, especially expedited mail, mass mailings, mailing lists, and couriers, and seek opportunities to implement cost-effective improvements and/or to enhance performance of the agency's mission;

(d) Develop and direct agency programs and plans for proper and cost-effective use of transportation, equipment, and supplies used for mail;

(e) Although not required for other than large agencies, develop, implement and provide to GSA the agency's annual mail management and mail security plan (see subpart C) of this part;

(f) Ensure that facility mail managers receive the training they need to perform their assigned duties;

(g) Ensure that users at the program level receive the training needed to reduce, track and budget for their mailing expenses;

(h) Ensure that expedited mail and couriers are used only when authorized by the Private Express Statutes (39 U.S.C. 601–606) and when necessary and cost-effective;

(i) Establish written policies and procedures to minimize personal mail in incoming, outgoing, and internal agency mail;

Note to paragraph (i): An agency may decide to accept and process personal mail for personnel living on a Federal facility, personnel stationed outside the United States, or personnel in other situations who would otherwise suffer hardship. Mailing costs associated with filing travel vouchers and payment of Government sponsored charge card billings are considered as ''incidental expenses'' as defined in the ''Per Diem Allowance'' in the Federal Travel Regulations (41 CFR 300–3.1).

(j) Establish and maintain a system that tracks the financial and other performance data discussed in §§ 102–192.50 and 102–192.100;

(k) Work with agency executives to ensure that, to the maximum practical extent, the person who makes the decision to mail any significant number of pieces of mail is the same person who controls the funds for postage;

(l) Work with agency accounting personnel to ensure that financial

systems show allocations and expenses for postage and all other mail costs separately from all other administrative expenses; and

(m) Ensure that bills from all service providers are reconciled and paid on a timely basis.

Subpart G—Facility Mail Manager Responsibilities

§ 102–192.130 What are my general responsibilities as a facility mail manager?

As a Federal facility mail manager you should:

(a) Implement policies and procedures developed by the agency mail manager, including cost control procedures;

(b) Work to improve, streamline, and reduce the cost of mail practices and procedures by continually reviewing work processes throughout the facility and seeking opportunities for cost-effective change;

(c) Work closely with all facility personnel, especially the program level users who develop large mailings, to minimize postage and associated printing expenses through improved mail piece design, mail list management, electronic transmission of data in lieu of mail, and other appropriate measures; keeping current on new technologies that could be applied to reduce your mailing costs;

(d) Work with local managers to ensure that, to the maximum practical extent, the person who makes the decision to mail any significant number of pieces of mail is the same person who controls the funds for postage;

(e) Ensure that expedited mail and couriers are used only when authorized by the Private Express Statutes (39 U.S.C. 601–606) and when necessary and cost-effective;

(f) Provide centralized control of all mail processing activities at the facility, including all regularly scheduled, small package, and expedited service providers, couriers, equipment and personnel;

(g) Review unauthorized use, loss, or theft of postage, including any unauthorized use of penalty or commercial mail stamps, meter impressions or other postage indicia, and immediately report such incidents to the agency Inspector General, internal security office, or other appropriate authority;

(h) Provide training opportunities for all levels of agency personnel at the facility on cost-effective mailing practices for incoming, outgoing, internal mail and security;

(i) Ensure that outgoing mail meets all the standards established by your service provider(s) for weight, size, hazardous materials content, etc.;

(j) Produce and implement an agency mail management and mail security plan; and

(k) Respond to the requirements of this part.

§ 102–192.135 What should I include when contracting out all or part of the mail function?

Any contract for a mail function should require compliance with:

(a) This part;

(b) The Private Express Statutes (39 U.S.C. 601–606); and

(c) All agency policies, procedures, and plans, including the agency wide mail management and mail security plan and, if applicable, facility mail security plans.

Subpart H—Program-Level Mail Responsibilities

§ 102–192.140 Which program levels should have a mail manager?

Every program level within a Federal agency that generates a significant quantity of outgoing mail should have a mail manager at the program level. It is up to each agency to decide which programs will have a full-time or part-time mail manager. In making this determination, the agency should consider the total volume of outgoing mail that is put into the mail stream by the program itself or by a printer, presort contractor, or other contractor on the program's behalf.

§ 102–192.145 What are the mail responsibilities at the program level?

Your responsibilities at the program level include:

(a) Ensuring that your program complies with all applicable mail policies and procedures, including this part;

(b) Working closely with your program personnel to minimize postage and associated printing expenses through improved mail piece design, mail list management, electronic transmission of data in lieu of mail, and other appropriate measures;

(c) Keeping current on new technologies and practices that could reduce your mailing costs and/or make your use of mail more effective;

(d) Coordinating all of your program's large mailings and print jobs to ensure that the most efficient and effective procedures are used;

(e) Providing training opportunities to your program personnel; and

(f) Working closely with the agency mail manager, mail managers at all agency facilities that handle significant quantities of mail or print functions for your program, and mail technical experts.

Subpart I—GSA's Responsibilities and Services

§ 102–192.150 What are GSA's responsibilities in mail management?

Under the Federal Records Management Amendments of 1976, as amended (44 U.S.C 2904), GSA is required to provide guidance and assistance to Federal agencies to ensure economical and effective records management by such agencies (mail is one type of record, according to the Act). In carrying out its responsibilities under the Act, GSA is required to:

(a) Promulgate standards, procedures, and guidelines;

(b) Conduct research to improve practices and programs;

(c) Collect and disseminate information on training programs, technological developments, etc.;

(d) Establish an interagency committee (*i.e.,* the Interagency Mail Policy Council) to provide an exchange of information among Federal agencies;

(e) Conduct studies, inspections, or surveys;

(f) Promote economy and efficiency in the selection and utilization of space, staff, equipment, and supplies; and

(g) In the event of an emergency, communicate with agencies.

§ 102–192.155 What types of support does GSA offer to Federal agency mail management programs?

GSA supports Federal agency mail management programs by:

(a) Assisting development of agency policy and guidance in mail management and mail operations;

(b) Identifying better business practices and sharing them with Federal agencies;

(c) Developing and providing access to a Governmentwide management information system for mail;

(d) Helping agencies develop performance measures and management information systems for mail;

(e) Maintaining a current list of Agency Mail Managers;

(f) Establishing, developing and maintaining interagency mail committees;

(g) Maintaining liaison with the USPS and other service providers at the national level;

(h) Maintaining a website for mail communications policy; and

(i) Serving as a point of contact for mail issues. You may also contact GSA at: General Services Administration, Office of Governmentwide Policy, Mail Communications Policy Division (MTM), 1800 F Street, NW., STE 1221,

Washington, DC 20405; e-mail: *federal.mail@gsa.gov.*

Appendix A To Part 102–192—Large Agency Mailers

As of December 2000, the following 26 large agencies met the definition of ''large agency'' in § 102–192.35:

Department of Agriculture
Department of Commerce
Department of Defense
Department of Education
Department of Energy
Department of Health and Human Services
Department of Housing and Urban Development
Department of Interior
Department of Justice
Department of Labor
Department of State
Department of Transportation
Department of Treasury
Department of Veterans Affairs
Environmental Protection Agency
Equal Employment Opportunity
Federal Deposit Insurance Corporation
Federal Emergency Management Agency
General Services Administration
Government Printing Office
Library Of Congress
National Aeronautics and Space Administration
National Science Foundation
Small Business Administration
Smithsonian Institution
Social Security Administration

Appendix B To Part 102–192—Mail Center Security Plan

Introduction

I. The mail center is a major gateway into any business or government agency. Each day, the typical mail center handles hundreds or thousands of items from routine letters to confidential documents, high value parcels, and even money. Security is critical for this critical nerve center. An effective mail center security program should address:

A. Risk Analysis
B. Employee Safety
C. Physical Security
D. Inbound Mail Procedures
E. Postage Security
F. Contractors
G. Continuity of Operations Planning
H. Communications
I. Training
J. Plan Review

II. Some agencies have satellite locations with no official mail centers. Responsibilities for processing mail are divided among administrative and support staff. Although the security plan for mail operations may be limited for these smaller sites, each of the sections A. through J. of the appendix should be adopted when appropriate.

III. A strong plan supplemented with regular training and reviews will help instill a culture that emphasizes the importance of good security. Maximize the success of the security plan by involving all members of your team—managers, employees, security managers and union representatives—during development.

A. Risk Analysis

The first step in effective security is to conduct a risk analysis for your mail operation. While there are minimum standards that every agency should follow, your particular posture should reflect the mission of your agency.

B. Employee Safety

The anthrax attacks reminded us all how important employee safety is. We do not know whether there will be another attack, so we should take the proper steps to ensure the safety of our employees.

1. Personal protection equipment should be made available for all employees. These include gloves and masks. When using any form of respiratory equipment, the manager must make sure that proper OSHA standards are met. *See* appendix D of OSHA's Respiratory Protection standard for information about the use of respirators when such use is voluntary (29 CFR 1910.134, appendix D).

2. Also, instruct employees to wash hands regularly with soap and water. At a minimum, hands should be washed when gloves are removed, before eating, and at the end of a shift.

C. Physical Security

Managers need to address the physical security of the mail center.

1. Place the mail center in an enclosed room, with defined points of entry. Limit access to those employees who work in the mail center, or who have immediate need for access, such as known couriers.

2. Where appropriate, install controlled access equipment; key control, card readers or buzz entry are a few options. Additionally, each access point should be alarmed and monitored for after hours activity. Secure areas, such as safes or locked cabinets, should be established inside the mail center for meters, express shipments and valuables.

3. Managers should draft detailed procedures for opening and closing the mail center. Logs with checklists should be posted and signed daily.

D. Inbound Mail Procedures

1. The inbound mail operation should be separate from the rest of the mail center. All incoming mail should be isolated in an area where it can be inspected. Delivery personnel should have limited access to the facility and should be serviced at a counter.

2. Establish a closed-loop manifest system for all accountable letters and packages (e.g., certified mail, UPS, FedEx). Verify the delivery manifest sheet to ensure that you have received all packages listed. All accountable mail should be signed for whenever possession changes. Always require a signature at the final point of delivery. File copies of the manifest by date.

3. If possible, acquire an x-ray machine to scan mail. All mail, regardless of carrier, should be x-rayed. If volume does not permit this, x-ray all packages.

4. Mail center employees should be trained to recognize and report suspicious packages. Characteristics of a suspicious package or letter can vary depending upon the type of mail your operation regularly processes (see http://www.fbi.gov/pressrel/pressrel01/mail3.pdf for more information).

E. Postage Security

Postage theft is a Federal offense and managers should be proactive in this area.

1. Managers should integrate accounting procedures for all forms of postage—meters, stamps and permits. Meter logs must be accurately kept, and meters should be locked when not in use. Where feasible, the meter should be removed from the equipment and stored in a locked cabinet during off-hours.

2. Establish additional controls to ensure proper access and accountability for permit envelopes and labels. Controls should be established for stamps and other carriers as well.

F. Contractors

Some agencies use contractors to process their mail. This could be either an outsource provider that runs your mail center or a lettershop that handles your presort. It's important to remember that security of the mail is still the responsibility of the agency. Include the key points from your security plan in every contract, and conduct periodic reviews separate from the contract process.

G. Continuity of Operations Planning

1. Managers should have a written continuity of operations plan (COOP) to deal with emergency situations. The plan should include:

a. Name(s) of Mail Security Coordinator/Response Team
b. Procedures on how to respond to a threat or incident
c. Who to contact in the event of an emergency
d. Location and contents of ''fly-away kit''
e. Location/phone numbers of backup facility
f. A list of critical documents and mail required for the agency to complete its mission

2. Copies of this plan should be stored in easily accessible areas, including off-site.

3. Also, you need to test the plan on a quarterly basis. Verify that all the information is up-to-date, that contacts, facilities access, and the call trees are correct.

H. Communications

A good communications program is part of any successful mail operation and is critical for security issues. Make sure that the information being shared is factual, not opinion, and verify that it is up-to-date.

1. Schedule regular meetings with a representative from the senior management of your agency (Executive Secretariat, Administrator, *etc.*). Review the steps you've taken to secure the mail, and address any outstanding issues.

2. Develop a communications plan to be executed when responding to a threat. This plan should cover how to both acquire and distribute information. Prepare a list of trusted resources to acquire timely and accurate information (*e.g.*, GSA, USPS, CDC, *etc.*). Organize a protocol for the approval and distribution of information on the status of the mail operation.

I. Training

Education and awareness are the essential ingredients to preparedness. Employees must remain aware of their surroundings and the packages they handle. You must carefully design and vigorously monitor your security program to reduce the risk for all.

1. Through training you can develop a culture of security awareness in your operation. Essential to ensuring employee confidence in their safety is the inclusion of union representatives or other employee representatives in developing and giving training. Managers should consider security training a critical element of their job.

2. A complete training program will include:

a. Basic security procedures;

b. Recognizing and reporting suspicious packages;

c. Proper use of personal protection equipment;

d. Responding to a biological threat; and

e. Responding to a bomb threat.

3. Maintain a log of all employees and training attended, including the date completed. Follow up with refresher training on a regular basis.

4. In addition to educating the employees who work for you, you must educate all employees who work in the facility on best mail practices including security measures. Employee awareness of the measures you have taken leads to confidence in the safety of the packages that are delivered to their desktops.

J. Plan Review

The General Services Administration strongly recommends external review of your security plan. This may include a review by a consultant, your agency security department, or a peer review.

Dated: May 16, 2002.

Stephen A. Perry,

Administrator of General Services.

[FR Doc. 02–13834 Filed 6–5–02; 8:45 am]

BILLING CODE 6820–24–P

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 15

[ET Docket No. 95–177; FCC 02–135]

Biomedical Telemetry Transmitters

AGENCY: Federal Communications Commission.

ACTION: Final rule; denial.

SUMMARY: This document dismisses a petition for reconsideration filed by the Cellular Phone Taskforce concerning the effects of radio frequency radiation on ''electrosensitive'' individuals, and denies a petition for partial reconsideration concerning separation distances filed by the National Association of Broadcasters.

FOR FURTHER INFORMATION CONTACT: Hugh Van Tuyl, Office of Engineering and Technology, (202) 418–7506.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's *Memorandum Opinion and Order,* ET Docket No. 95–177, FCC 02–135, adopted May 2, 2002, and released May 13, 2002. The full text of this document is available for inspection and copying during regular business hours in the FCC Reference Center (Room CY–A257), 445 12th Street, SW, Washington, DC 20554. The complete text of this document also may be purchased from the Commission's copy contractor, Qualex International, 445 12th Street, SW., Room, CY–B402, Washington, DC 20554. The full text may also be downloaded at: *www.fcc.gov.* Alternative formats are available to persons with disabilities by contacting Brian Millin at (202) 418–7426 or TTY (202) 418–7365.

Summary of the Memorandum Opinion and Order

1. In October 1997, the Commission adopted a Report and Order (R&O) that increased the maximum permitted signal strength for medical telemetry transmitters operating in the broadcast television bands under Part 15 of the rules. The R&O also permitted these devices to operate on TV channels 14–46 in addition to TV channels 7–13 where they already were permitted to operate. To prevent interference to TV broadcast signals, minimum required separation distances were established between medical telemetry transmitters and the Grade B contours of co-channel analog TV stations. No separation distances were proposed or established between medical telemetry transmitters and the noise limited service contours of digital TV stations, but medical telemetry transmitters must operate on a non-interference basis to digital TV and to all other authorized services.

2. Two parties filed petitions for reconsideration of the rules adopted in the R&O. The Cellular Phone Taskforce (CPT) claims that the transmission levels permitted in the rules are too high and are therefore discriminatory because they will adversely affect persons who are extremely sensitive to electromagnetic fields. The National Association of Broadcasters (NAB) claims that the rules do not provide adequate protection to analog TV broadcast signals from interference caused by medical telemetry transmitters. NAB states that we used a desired-to-undesired (D/U) signal ratio that was too low in calculating the minimum required separation distances between medical telemetry transmitters and the Grade B contours of co-channel TV stations. NAB's petition did not address the issue of protecting digital TV signals from interference by medical telemetry equipment.

3. Prior to the adoption of the Report and Order in this proceeding, the Commission addressed in another proceeding CPT's arguments that stringent standards for RF emissions should be established to protect persons who are adversely affected by exposure to low-level electromagnetic fields. More specifically, in 1996, CPT filed a petition for reconsideration in ET Docket 93–62, which adopted new guidelines and methods for evaluating the environmental effects of radio frequency (RF) radiation from FCC-regulated transmitters. CPT's petition in that proceeding argued that stricter RF emission limits were necessary to protect persons who are ''electrosensitive.'' The Commission denied CPT's petition on August 25, 1997, stating that the RF safety rules adopted in that proceeding were based on the recommendations of expert organizations and federal agencies with responsibilities for health and safety, and that it was not practicable for the Commission to independently evaluate studies of biological effects, especially concerning controversial issues such as whether some persons are ''electrosensitive.'' CPT appealed the Commission's decision in ET Docket 93–62 at the same time it petitioned for reconsideration of the Commission's decision in this proceeding. The Court affirmed the Commission's decision to rely on standards formulated by expert organizations and agencies. In denying a rehearing, the Court specifically concluded, in response to CPT's claims of discrimination against handicapped persons, that the American with Disabilities Act (42 U.S.C. 12101 *et seq.*) did not apply to the Commission's decision and that arguments made under the Rehabilitation Act (29 U.S.C. 701 *et seq.*) were without merit. Because the essence of CPT's arguments here have already been addressed by the Commission in ET Docket 93–62 and the Commission's decision in that proceeding has been affirmed on appeal, we are dismissing CPT's petition for reconsideration in this proceeding.

4. We find that the 45 dB D/U signal ratio we selected to determine the required separation distances between medical telemetry transmitters and TV grade B contours is appropriate. This ratio was originally adopted by the Commission in 1952 to protect TV stations from interference from co-channel TV stations at the Grade B