

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.

## PART 102–193—CREATION, MAINTENANCE, AND USE OF RECORDS

Sec.

102–193.5 What does this part cover?

102–193.10 What are the goals of the Federal Records Management Program?