§ 102–192.70 What security policies and plans must we have?

(a) You must have a written mail security policy that applies throughout the agency.

(b) You also must have a written mail security plan for each facility that processes mail, regardless of the facility’s mail volume.

(c) If a contract that is in place on August 25, 2008 does not fully meet the requirements of this section, the contract must be modified to meet the requirement for a security plan within one year of August 25, 2008, unless the contract will expire prior to that date.

(d) The scope and level of detail of each facility mail security plan should be commensurate with the size and responsibilities of each facility. For small facilities, you may provide a general, standardized plan that is used in many similar locations. For larger locations, you must develop a plan that is specifically tailored to the threats and risks at your location. Agencies are free to determine for themselves which facilities are “smaller” and which are “larger” for the purposes of this section, so long as the basic requirement for a security plan is met at every facility.

(e) Mail facility managers should report annually the status of their facility mail security plans to agency headquarters. At a minimum, this report should assure that the facility mail security plan complies with the requirements of this part, including annual review by a subject matter expert and regular rehearsal of responses to various emergency situations by facility personnel.

(f) An outside security professional who has expertise in mail center security should review the agency’s mail security plan annually. Review of facility mail security plans can be accomplished by outside subject matter experts such as agency security personnel. If these experts are not available within your agency, seek assistance from the Postal Inspection Service or other Federal authorities.

§ 102–192.75 Why must we have written security policies and plans?

All Federal mail programs must identify, prioritize, and coordinate the protection of all mail processing facilities in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit the mail center or the national mail infrastructure. Homeland Security Presidential Directive HSPD-7 requires all agencies to protect key resources from terrorist attacks, and this is spelled out in the Postal and Shipping Sector Plan, which is part of the National Infrastructure Protection Plan (NIPP) prescribed by HSPD-7. All Federal mail centers are key resources under that plan. Details on the Postal and Shipping Sector Plan are not publicly available. Federal employees needing access to the plan should contact the Department of Homeland Security (DHS) at NIPP@dhs.gov.

§ 102–192.80 How do we develop written security policies and plans?

Agency mail managers must coordinate with their agency security service and/or the Federal Protective Service...
Federal Management Regulation

§ 102–192.90 What must we include in our annual mail management report to GSA?

Your annual report must—
(a) Identify your agency mail manager; in addition you must promptly report the name of the agency mail manager whenever there is a change of the person serving in this role.
(b) State the total amounts paid to each service provider during the previous fiscal year:
   (1) These amounts should include only amounts paid for mail; not amounts paid to any service provider to ship parts and supplies from a material distribution center (see the definition of mail in §102–192.30).
   (2) These amounts should include all postage costs associated with mailing printed materials, regardless of whether the printing is accomplished by the agency or a contractor, and regardless of how the postage expense is paid (e.g., GSA’s Federal Acquisition Service (FAS) produces a publication called “Marketips,” which provides information about supplies and services available through GSA sources. GSA should include the postage that it uses to mail Marketips in the amounts that it reports, even though a printing company actually prints and mails the publication);
(c) Report actual results for the performance measures in use at the agency and facility levels;
(d) Describe your agency’s accomplishments and plans to improve the economy and efficiency of mail operations in the current and future years;
(e) Identify how many Federal employees and contractors work in your agency’s mail operations nationwide, and the number that have achieved industry certifications (e.g., Certified Mail and Distributions Systems Manager, Mailpiece Quality Control Specialist, Certified Mail Manager);
(f) Describe your agency’s approach to ensuring that program level officials are accountable for postage; and
(g) Verify that a competent expert has reviewed your agency security policies and the mail security plan for each facility within the past year, or explain what steps your agency has taken in this regard.

Subpart D—Reporting Requirements

§ 102–192.85 Who must report to GSA annually?

Large agencies (all agencies that spend in excess of $1 million each fiscal year in total payments to mail service providers) must provide a Mail Management Report to GSA by January 15th of each year. If your agency is a cabinet-level or independent agency, the agency mail manager must compile all offices (or components) and submit one report for the department or agency as a whole (e.g., the Department of Defense or the Department of Health and Human Services).