

Subpart C—Security Requirements for All Agencies

§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) All 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 to develop agency mail security policies and plans. The Federal Protective Service has, working with the Interagency Security Committee which it chairs, developed standards for building construction and management, including standards for mail centers. At a minimum, the agency mail security plan must address the following topics—

- (a) Risk assessment;
- (b) Plan to protect staff and all other occupants of agency facilities from hazards that might be delivered in the mail;

- (c) Operating procedures;
- (d) Plan to provide a visible mail screening operation;
- (e) Training mail center personnel;
- (f) Testing and rehearsing responses to various emergency situations by agency personnel;
- (g) Managing threats;
- (h) Communications plan;
- (i) Occupant Emergency Plan (OEP);
- (j) Continuity of Operations Plan (COOP); and
- (k) Annual reviews.

Note to [102-192.80](#): The agency mail manager and facility manager(s) need not prepare all of these plans themselves. They should participate actively in the development and implementation of each of these elements, but other parts of the agency or outside security professionals should take the lead in their respective areas of expertise.