2 Audits and Investigations

21 General

211 Authority

211.1 Responsibility

211.11 Inspector General

211.12 Chief Inspector
The Postal Inspection Service, a federal law enforcement agency, conducts audits and investigations of Postal Service programs and operations (18 U.S.C. 3061 and 39 U.S.C. 404 (a)(7)), and is headed by the chief inspector, who reports directly to the postmaster general. The chief inspector acts as security officer and emergency coordinator for the Postal Service and maintains liaison with other investigative and law enforcement agencies of the government, as well as the Federal Emergency Management Agency and other emergency coordinators.

211.13 Designation of Functions
The Governors approved a distribution of duties and responsibilities between the OIG and the Postal Inspection Service to maximize each organization’s capabilities and maintain their legislated roles and responsibilities. The designations of functions provide for partnering opportunities, while avoiding duplicative efforts. See Exhibit 211 for a synopsis of the designation of functions.
Exhibit 211
Designation of Functions

<table>
<thead>
<tr>
<th>Office of Inspector General*</th>
<th>Postal Inspection Service</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Audits</strong></td>
<td></td>
</tr>
<tr>
<td>- Financial statements,</td>
<td>- Financial statements,</td>
</tr>
<tr>
<td>including:</td>
<td>including installations</td>
</tr>
<tr>
<td>- Overall opinion audits</td>
<td>and districts</td>
</tr>
<tr>
<td>- Quality reviews of</td>
<td></td>
</tr>
<tr>
<td>Postal Inspection Service</td>
<td></td>
</tr>
<tr>
<td>- Postal-wide performance</td>
<td>- Area, district and</td>
</tr>
<tr>
<td>reviews</td>
<td>local performance</td>
</tr>
<tr>
<td>- Contract audits,</td>
<td>- Service investigations</td>
</tr>
<tr>
<td>except pre-award and</td>
<td>- Pre-award and post-award</td>
</tr>
<tr>
<td>post-award audits</td>
<td>contract audits</td>
</tr>
<tr>
<td>- Developmental audits</td>
<td></td>
</tr>
<tr>
<td>- Facility audits,</td>
<td>- Facility audits,</td>
</tr>
<tr>
<td>including:</td>
<td>- Facilities construction</td>
</tr>
<tr>
<td>- Facilities construction</td>
<td>contracts of $5 million</td>
</tr>
<tr>
<td>contracts of $10 million</td>
<td>or less</td>
</tr>
<tr>
<td>- Right of first choice</td>
<td>- Contracts between</td>
</tr>
<tr>
<td>on contracts valued</td>
<td>$5–10 million not</td>
</tr>
<tr>
<td>between $5–10 million</td>
<td>performed by OIG</td>
</tr>
<tr>
<td>- Leases of $1 million or</td>
<td>- Leases under $1 million</td>
</tr>
<tr>
<td>more</td>
<td>- Repair and alterations</td>
</tr>
<tr>
<td>- Repair and alterations</td>
<td>under $1 million</td>
</tr>
<tr>
<td>of $1 million or more</td>
<td></td>
</tr>
<tr>
<td>- Revenue-focused audits</td>
<td></td>
</tr>
<tr>
<td>(international mail)</td>
<td></td>
</tr>
<tr>
<td><strong>Investigations</strong></td>
<td></td>
</tr>
<tr>
<td>- Revenue cases, including:</td>
<td>- Revenue cases, including:</td>
</tr>
<tr>
<td>- Bribery, kickbacks,</td>
<td>- Revenue loss detection</td>
</tr>
<tr>
<td>conflicts of interest</td>
<td>- Shares with OIG on</td>
</tr>
<tr>
<td>- Systemic reviews</td>
<td>revenue task force and</td>
</tr>
<tr>
<td>- Workers’ compensation</td>
<td>other groups</td>
</tr>
<tr>
<td>cases, including:</td>
<td></td>
</tr>
<tr>
<td>- Inspector General</td>
<td>- Primary responsibility</td>
</tr>
<tr>
<td>subpoenas</td>
<td>for workers’ compensation</td>
</tr>
<tr>
<td>- Program monitoring</td>
<td>cases</td>
</tr>
<tr>
<td>- Tort claims, including:</td>
<td>- Tort claims</td>
</tr>
<tr>
<td>- Serious incidents</td>
<td></td>
</tr>
<tr>
<td>- Liability reports</td>
<td></td>
</tr>
<tr>
<td>- Embezzlements (conduct/</td>
<td>- Embezzlements under $100,</td>
</tr>
<tr>
<td>partner on cases of $100,</td>
<td>000 or more)</td>
</tr>
<tr>
<td>000 or more)</td>
<td></td>
</tr>
<tr>
<td>- Expenditure cases,</td>
<td>- Expenditure cases,</td>
</tr>
<tr>
<td>including:</td>
<td>- Cases referred by OIG</td>
</tr>
<tr>
<td>- Bribery, kickbacks,</td>
<td>- IMPAC card cases</td>
</tr>
<tr>
<td>and conflicts of interest</td>
<td>- Local purchases or</td>
</tr>
<tr>
<td>- Systemic reviews</td>
<td>procurements</td>
</tr>
<tr>
<td>- Conduct/partner on cases</td>
<td>- Conduct/partner on cases</td>
</tr>
<tr>
<td>involving executives</td>
<td>involving executives</td>
</tr>
<tr>
<td>- Postal Inspection Service</td>
<td>- Emergency responses on</td>
</tr>
<tr>
<td>internal affairs:</td>
<td>cases involving</td>
</tr>
<tr>
<td>executives</td>
<td>executives</td>
</tr>
<tr>
<td>- Computer forensics</td>
<td>- Internal and external</td>
</tr>
<tr>
<td>- Hotline</td>
<td>crimes</td>
</tr>
<tr>
<td><strong>Other</strong></td>
<td></td>
</tr>
<tr>
<td>- Oversight of the</td>
<td>- Employee protection</td>
</tr>
<tr>
<td>Postal Inspection Service</td>
<td>- Security</td>
</tr>
<tr>
<td>- Postal rate-making</td>
<td>- Fraud and prohibited</td>
</tr>
<tr>
<td>programs and operations</td>
<td>mailings</td>
</tr>
<tr>
<td>- Revenue generation</td>
<td>- Postal Inspection Service</td>
</tr>
<tr>
<td>- Labor management</td>
<td>internal affairs:</td>
</tr>
<tr>
<td>- Electronic commerce</td>
<td>non-executives</td>
</tr>
<tr>
<td>- Forensic and technical</td>
<td></td>
</tr>
<tr>
<td>services</td>
<td>- Hotline</td>
</tr>
</tbody>
</table>

* The Inspector General has oversight responsibility for Postal Inspection Service functions. The Inspector General retains the right to conduct/partner with the Postal Inspection Service on audits and investigations, pursuant to the Inspector General Act.
211.14  **Federal Laws and Postal Regulations**

211.141 The OIG is responsible for promoting economy, efficiency, and effectiveness, and preventing and detecting fraud, waste, and abuse in all postal programs and operations. The OIG conducts and supervises audits, evaluations, and investigations and keeps the Governors and Congress fully informed of problems and deficiencies and the progress of corrective actions. Under applicable policies, regulations, and procedures, it carries out investigations and presents evidence to the Department of Justice and U.S. attorneys in investigations of a criminal nature.

211.142 The Postal Inspection Service is responsible for protection of the mails, enforcement of federal laws and postal regulations within its jurisdiction as provided in 211.22, plant and personnel security, and coordinating Postal Service emergency preparedness planning of both a wartime and a natural disaster nature. The Postal Inspection Service, under applicable policies, regulations, and procedures, carries out investigations and presents evidence to the Department of Justice and U.S. attorneys in investigations of a criminal nature. In coordination with the OIG, the Postal Inspection Service also performs selected audits and reviews of the Postal Service.

211.2  **Arrest and Subpoena Powers**

211.21  **Authorization**

OIG special agents and postal inspectors are authorized to perform the following functions in connection with any matter within their respective official duties as established by the inspector general and the chief inspector:

a. Carry firearms.

b. Serve warrants and subpoenas issued under the authority of the United States.

c. Make arrests without warrant for offenses against the United States committed in their presence.

d. Make arrests without warrant for felonies cognizable under the laws of the United States, if they have reasonable grounds to believe that the person to be arrested has committed or is committing such a felony.

211.22  **Limitations**

The powers granted by 211.21 are exercised only in the enforcement of laws regarding property in the custody of the Postal Service, property of the Postal Service, the use of the mails, other postal offenses, and pursuant to any agreements between the attorney general and the Postal Service, in the enforcement of other federal laws, violations of which the attorney general determines have a detrimental effect on the Postal Service.
211.3 Access to Records

211.31 Records and Documents
The OIG and Postal Inspection Service are authorized access to all records and documents of possible relevance to an official audit, evaluation, fact-finding, inspection, investigation, review or other inquiry whether they are in the custody of the Postal Service or otherwise available to the Postal Service by law, contract, or regulation. This includes information about mail sent or received by a particular customer. Exceptions to authorized access are listed in 211.33.

211.32 Disclosure
Information obtained under 211.31 may be disclosed to other postal employees who have a need for such information in the performance of their duties or to any federal, state, or local government agency or unit thereof that needs such information for civil, administrative, or criminal law enforcement. Any such disclosure must be consistent with Postal Service privacy regulations (see 353).

211.33 Exceptions
There are no exceptions when an inquiry, such as an investigation, inspection, evaluation, fact-finding, review, or audit is conducted under the authority of the Inspector General Act. Exceptions to the policy of disclosure are the following:

a. For information from the covers of mail, see 213. For dead mail, see the Domestic Mail Manual.

b. For access to employee restricted medical records and Employee Assistance Program records, see Handbook EL-806, Health and Medical Service, Chapter 2, and Employee and Labor Relations Manual (ELM) 870.

c. For access to an employee’s Form 2417, Confidential Statement of Employment and Financial Interests, see the ELM or 39 CFR 447.42(e)(2).

212 Circulars and Rewards

212.1 Wanted Circulars
The Postal Inspection Service and the OIG issues wanted circulars to help locate and arrest fugitive postal offenders. Post these circulars in the most conspicuous place in the post office lobby and in other prominent places. Post near Poster 296, Notice of Reward. Telephone immediately the postal inspector in charge or inspector general with any information on the possible location of the person wanted. Remove and destroy circulars immediately when notified of their cancellation or when the circular is not listed in the periodic Postal Bulletin notices of current wanted circulars.
212.2 **Rewards**

212.21 **Criminal Postal Offenses**

Rewards are paid, in the amounts and under the conditions stated in Poster 296, for the arrest and conviction of persons for these postal offenses:

a. Robbery or attempted robbery.

b. Mailing bombs, explosives, poison, or controlled substances.

c. Post office burglary.

d. Stealing or unlawfully possessing mail, money, or property of the United States under Postal Service custody or control, including Postal Service property.

e. Destroying, obstructing, or retarding the passage of mail.

f. Altering, counterfeiting, forging, unlawful uttering, or passing of postal money orders; or unlawfully using, counterfeiting, or forging of postage stamps or other postage; or using, selling, or possessing with intent to use or sell any forged or counterfeit postage stamp or other postage; or misusing of postage meters.

g. Assaulting a postal employee.

h. Committing the murder or manslaughter of a postal employee.

i. Mailing or receiving through the mail any visual depiction involving a minor engaging in sexually explicit conduct.

212.22 **Other Rewards**

The chief inspector and/or the inspector general may pay a reward for information leading to the detection of people or firms who obtain or secure postal funds, property, or services based on false or fraudulent activities, statements, or claims. The reward amount may not exceed one-half of the amount collected by the Postal Service from funds recovered through civil or criminal proceedings.

212.23 **Reward Notices**

The postmaster or a designated employee should present reward notices to representatives of firms transporting mail, security or detective units of firms, police officers, sheriffs and their deputies, if practicable, and encourage their cooperation in protecting mail and Postal Service property.

213 **Mail Covers**

213.1 **Policy**

The Postal Service maintains rigid controls and supervision with respect to the use of mail covers as an investigative technique for law enforcement or the protection of national security.
213.2 Scope

These regulations constitute the sole authority and procedure for initiating a mail cover, and for processing, using, and disclosing information obtained from mail covers.

213.3 Definitions

The following definitions apply to mail covers:

a. **Mail cover** is the process by which a nonconsensual record is made of any data appearing on the outside cover of any sealed or unsealed class of mail matter (see 274.23), or by which a record is made of the contents of unsealed class of mail matter as allowed by law, to obtain information for any of the following:
   (1) Protecting national security.
   (2) Locating a fugitive.
   (3) Obtaining evidence of commission or attempted commission of a crime.
   (4) Obtaining evidence of a violation or attempted violation of a postal statute.
   (5) Assisting in the identification of property, proceeds, or assets forfeitable under law.

b. **Record**, for the purposes of this section, is a transcription, photograph, photocopy, or any other facsimile of the image of the outside cover, envelope, wrapper, or contents of any class of mail.

c. **Sealed matter** is mail on which appropriate postage is paid, and which under postal laws and regulations is included within a class of mail maintained by the Postal Service for the transmission of mail sealed against inspection, including First-Class Mail, Priority Mail, Express Mail, international letter mail forming part of the LC class of Postal Union mail, and mailgram messages.

d. **Unsealed mail** is mail on which appropriate postage for sealed mail has not been paid and which under postal laws or regulations is not included within a class of mail maintained by the Postal Service for the transmission of mail sealed against inspection. Unsealed mail includes Periodicals, Standard Mail, incidental First-Class Mail attachments or enclosures, international parcel-post mail, the AO class of Postal Union mail, and the international post cards forming part of the LC class of Postal Union mail.

e. **Fugitive** is any person who has fled from the United States or any state, the District of Columbia, territory, or possession of the United States, to avoid prosecution for a crime, to avoid punishment for a crime, or to avoid giving testimony in a criminal proceeding.

f. **Crime**, for the purposes of this section, is any commission of an act or the attempted commission of an act punishable by law by imprisonment for a term exceeding 1 year.
g. *Postal statute* refers to a statute describing criminal activity, regardless of the term of imprisonment, for which the Postal Service has investigative authority, or which is directed against the Postal Service, its operations, programs, or revenues.

h. *Law enforcement agency* is any authority of the federal government or any authority of a state or local government, one of whose functions is to investigate the commission or attempted commission of acts constituting a crime, or protect the national security.

i. *Protection of the national security* means to protect the United States from any of the following actual or potential threats to its security by a foreign power or its agents:

   (1) An attack or other grave hostile act, including upon information infrastructures.
   (2) Sabotage or international terrorism.
   (3) Clandestine intelligence activities, including commercial espionage.

j. *Emergency situation* refers to circumstances that require the immediate release of information to prevent the loss of evidence or in which there is a potential for immediate physical harm to persons or property.

213.4 **Authorizations**

213.41 **Chief Postal Inspector**

The chief postal inspector is the principal officer of the Postal Service in the administration of all matters governing mail covers.

213.42 **Delegation of Authority**

The chief postal inspector may delegate any or all authority in this regard to the deputy chief inspectors at Postal Inspection Service Headquarters.

213.43 **ISOSG Managers and Inspectors in Charge**

Except for national security mail covers, the chief postal inspector also may delegate any or all authority to the Postal Inspection Service Operations Support Group (ISOSG) managers, and, for emergency situations, to inspectors in charge. The ISOSG managers may delegate this authority to no more than two designees.

213.44 **Directives**

Delegations of authority are issued through official, written directives. Except for delegations at Postal Inspection Service Headquarters, such delegations apply only to the geographic areas served by the ISOSG managers, or their designees.
213.5 Ordering Mail Covers

The chief postal inspector or designee may order mail covers under any of the following circumstances:

a. When a written request is received from a postal inspector or OIG special agent that states reason to believe a mail cover will produce evidence relating to the violation of a postal statute.

b. When a written request is received from any law enforcement agency in which the requesting authority specifies the reasonable grounds to demonstrate the mail cover is necessary to: protect the national security, locate a fugitive, obtain information regarding the commission or attempted commission of a crime, or assist in the identification of property, proceeds, or assets forfeitable because of a violation of criminal law.

c. When time is of the essence, the chief inspector or designee may act on an oral request, to be confirmed by the requesting authority in writing within 3 calendar days. Information may be released by the chief postal inspector or designee, prior to receipt of written request, only when the releasing official is satisfied that an emergency situation exists.

213.51 ISOSG Managers

213.511 Circumstances

All five ISOSG managers or their designees pursuant to delegations in writing, may order mail covers within their geographic jurisdiction under either of the following circumstances:

a. When there is reason to believe that the subject or subjects are engaged in an activity violating any postal statute.

b. When written request is received from any law enforcement agency of the federal, state, or local governments in which the requesting authority stipulates and specifies the reasonable grounds that demonstrate that the mail cover either would aid in locating a fugitive or obtaining information about the commission or attempted commission of a crime.

213.512 Approvals

Except when ordered by the chief inspector or designee, requests for mail covers must be approved by the ISOSG manager or designee in each locale in which the mail cover is to operate.

213.6 Exceptions

A postal inspector or a postal employee acting at the direction of a postal inspector may record the information appearing on the envelope or outer wrapping of mail without obtaining a mail cover order only under the following circumstances:

a. Undelivered mail found abandoned or in the possession of a person reasonably believed to have stolen or embezzled such mail.
b. Damaged or rifled, undelivered mail.

c. Mail that poses an immediate threat to persons or property.

213.7 Limitations

The following limitations apply:

a. Mail covers only authorize the recording of mail information for a law enforcement investigative purpose. Mail may only be detained, opened, searched, and seized in accordance with section 274. Information from mail may be recorded for operational purposes as prescribed by section 274.5.

b. No mail cover shall include matter mailed between the mail cover subject and the subject’s known attorney.

c. No officer or employee of the Postal Service other than the chief postal inspector, ISOSG manager, and their designees are authorized to order mail covers. Under no circumstances may a postmaster or postal employee furnish information for a law enforcement purpose, except as authorized by a mail cover order issued by the chief postal inspector or designee, or as directed by a postal inspector under the circumstances described in 213.6.

d. Except for mail covers ordered upon fugitives or subjects engaged, or suspected to be engaged, in any activity against the national security, no mail cover order shall remain in effect for more than 30 days, unless adequate justification is provided by the requesting authority. At the expiration of the mail cover order period, or prior thereto, the requesting authority may be granted additional 30-day periods under the same conditions and procedures applicable to the original request. The requesting authority must provide a statement of the investigative benefit of the mail cover and anticipated benefits to be derived from its extension.

e. No mail cover shall remain in force longer than 120 continuous days unless personally approved for further extension by the chief postal inspector or designees at Headquarters.

f. Except for fugitive cases, no mail cover shall remain in force when information has been filed or the subject has been indicted for the matter for which the mail cover is requested. If the subject is under investigation for further criminal violation, or a mail cover is required to assist in the identification of property, proceeds, or assets forfeitable because of a violation of criminal law, a new mail cover order must be requested consistent with these regulations.

g. Any national security mail cover request must be approved personally by the head of the law enforcement agency requesting the cover or one designee at the agency’s headquarters level. The head of the agency shall notify the chief postal inspector in writing of such designation.
213.8 **Records, Reports, and Review**

213.8.1 **Records**

All requests for mail covers, with records of action ordered thereon, and all reports issued pursuant thereto, shall be deemed within the custody of the chief postal inspector. However, the physical storage of this data shall be at the discretion of the chief postal inspector. The following also apply:

a. If the chief postal inspector or designee determines a mail cover was improperly ordered, all data acquired while the cover was in force shall be destroyed, and the requesting authority notified of the discontinuance of the mail cover and the reasons for it.

b. Any data concerning mail covers shall be made available to any mail cover subject in any legal proceeding through appropriate discovery procedures.

c. The retention period for files and records pertaining to mail covers is 5 years.

213.8.2 **Reporting to Requesting Authority**

Once a mail cover is duly ordered, authorization may be delegated to any employee in the Postal Inspection Service to transmit mail cover reports directly to the requesting authority.

213.8.3 **Review By Inspector General**

The inspector general or designee of the OIG oversight group periodically reviews mail cover orders issued by the Postal Inspection Service to ensure compliance with these regulations and procedures. The inspector general also selects and appoints a designee to conduct a periodic review of national security mail cover orders.

213.9 **Military Postal System**

Section 213 does not apply to the military postal system overseas or to persons performing military postal duties overseas. Information about regulations prescribed by the Department of Defense for the military postal system overseas may be obtained from the Department of Defense.

214 **Forfeitures**

214.1 **Authorization**

The Postal Service is authorized to seize property and conduct civil administrative forfeitures under any of the following:

a. 18 U.S.C. 981 (Civil Forfeiture).

b. 18 U.S.C. 982 (Criminal Forfeiture).

c. 18 U.S.C. 2251 et seq. (Child Protection Act).


e. 31 U.S.C. 5313(a) and 5324(a) (Currency Transaction Violations), Financial Institutions.
215 Audits and Investigations


215 Mail Fraud Investigations

The Postal Inspection Service has primary responsibility for investigating violations of the mail fraud laws. Consumer complaints are the primary basis for these investigations. Postal officials should send all consumer complaints, inquiries, or concerns relating to possible violations of the mail fraud or false representation statutes to the Postal Inspection Service Operations Support Group according to the ZIP Code of the subject of the complaint, based on the ranges shown in the table below. Matters not relating to mail fraud should be sent to the appropriate Postal Inspection Service Division.

| Divisions: | Gulf Coast, Miami, Michiana, Midwest, Northern California, Northern Illinois, Northwest, Rocky Mountain, Southeast, Southern California, Southwest, Tampa, Western Allegheny (except Pittsburgh) |
| Inclusive ZIP Codes: | 30001–37619, 37626–99999 |

| Divisions: | Mid-Atlantic, Newark, New York Metro, Northeast, Philadelphia Metro, San Juan, Washington Metro, Western Allegheny (Pittsburgh only) |
| Inclusive ZIP Codes: | 00001–29999, 37620–37625 |

FRAUD COMPLAINT SUPERVISOR
INSPECTION SERVICE OPERATIONS SUPPORT GROUP
2 GATEWAY CENTER FLOOR 9
NEWARK NJ 07175-0003

FRAUD COMPLAINT SUPERVISOR
INSPECTION SERVICE OPERATIONS SUPPORT GROUP
222 S RIVERSIDE PLAZA STE 1250
CHICAGO IL 60606-6100
22 Postal Emergencies, Losses, and Offenses

221 General Reporting Requirements

221.1 Reports
Postmasters must report emergencies, postal losses, and offenses to the Postal Inspection Service or the OIG.

221.11 Postal Inspection Service
Address reports of emergencies and other losses and offenses to the inspector in charge of the division where they took place (see Exhibit 221.11), except as required by 221.12.

221.12 Office of Inspector General
Address reports of embezzlements of $100,000 or more, and offenses involving postal career executive service managers to the OIG.

OFFICE OF INSPECTOR GENERAL
ATTN HOTLINE
1735 N LYNN STREET
ARLINGTON VA 22209-2020

Telephone: 888-USPS-OIG (888-877-7644)
Fax: 703-248-2259
E-mail: Hotline@uspsoig.gov

221.2 Emergencies
Report emergencies such as civil disorders, catastrophes, and disasters to the local postal inspector by telephone, confirming the report in writing to the Postal Inspection Service. Report any loss, damage, or casualty sustained (see 222).

221.3 Postal Losses and Offenses and National Defense Material
Report directly to the local postal inspector all cases of arson, burglary, assault, robbery, or explosion, or any classified national defense material found loose in the mail. Confirm the report in writing. Also inform local law enforcement officers of any of the above, except finding classified matter.
Exhibit 221.11  
Addresses of Postal Inspectors in Charge

<table>
<thead>
<tr>
<th>Division</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. CINCINNATI DIVISION</td>
<td>UNITED STATES POSTAL INSPECTION SERVICE 895 CENTRAL AVE STE 400</td>
</tr>
<tr>
<td></td>
<td>CINCINNATI OH 45202-5748</td>
</tr>
<tr>
<td>2. FLORIDA DIVISION</td>
<td>UNITED STATES POSTAL INSPECTION SERVICE 3400 LAKESIDE DR 6TH FL</td>
</tr>
<tr>
<td></td>
<td>MIRAMAR FL 33027-3242</td>
</tr>
<tr>
<td>3. GULF COAST DIVISION</td>
<td>UNITED STATES POSTAL INSPECTION SERVICE PO BOX 1276</td>
</tr>
<tr>
<td></td>
<td>HOUSTON TX 77251-1276</td>
</tr>
<tr>
<td>4. MICHIANA DIVISION</td>
<td>UNITED STATES POSTAL INSPECTION SERVICE PO BOX 330119</td>
</tr>
<tr>
<td></td>
<td>DETROIT MI 48232-6119</td>
</tr>
<tr>
<td>5. MID-ATLANTIC DIVISION</td>
<td>UNITED STATES POSTAL INSPECTION SERVICE PO BOX 3000</td>
</tr>
<tr>
<td></td>
<td>CHARLOTTE NC 28228-3000</td>
</tr>
<tr>
<td>6. MIDWEST DIVISION</td>
<td>UNITED STATES POSTAL INSPECTION SERVICE 1106 WALNUT ST</td>
</tr>
<tr>
<td></td>
<td>ST LOUIS MO 63199-2201</td>
</tr>
<tr>
<td>7. NEWARK DIVISION</td>
<td>UNITED STATES POSTAL INSPECTION SERVICE PO BOX 509</td>
</tr>
<tr>
<td></td>
<td>NEWARK NJ 07101-0509</td>
</tr>
<tr>
<td>8. NEW YORK METRO DIVISION</td>
<td>UNITED STATES POSTAL INSPECTION SERVICE PO BOX 555</td>
</tr>
<tr>
<td></td>
<td>NEW YORK NY 10116-0555</td>
</tr>
<tr>
<td>9. NORTHEAST DIVISION</td>
<td>UNITED STATES POSTAL INSPECTION SERVICE 425 SUMMER ST 7TH FLOOR</td>
</tr>
<tr>
<td></td>
<td>BOSTON MA 02210-1736</td>
</tr>
<tr>
<td>10. NORTHERN CALIFORNIA DIVISION</td>
<td>UNITED STATES POSTAL INSPECTION SERVICE PO BOX 882528</td>
</tr>
<tr>
<td></td>
<td>SAN FRANCISCO CA 94188-2528</td>
</tr>
<tr>
<td>11. NORTHERN ILLINOIS DIVISION</td>
<td>UNITED STATES POSTAL INSPECTION SERVICE 433 W HARRISON ST RM 50190</td>
</tr>
<tr>
<td></td>
<td>CHICAGO IL 60669-2201</td>
</tr>
<tr>
<td>12. NORTHWEST DIVISION</td>
<td>UNITED STATES POSTAL INSPECTION SERVICE PO BOX 400</td>
</tr>
<tr>
<td></td>
<td>SEATTLE WA 98111-4000</td>
</tr>
<tr>
<td>13. PHILADELPHIA METRO DIVISION</td>
<td>UNITED STATES POSTAL INSPECTION SERVICE PO BOX 7500</td>
</tr>
<tr>
<td></td>
<td>PHILADELPHIA PA 19101-9000</td>
</tr>
<tr>
<td>14. ROCKY MOUNTAIN DIVISION</td>
<td>UNITED STATES POSTAL INSPECTION SERVICE 1745 STOUT ST STE 900</td>
</tr>
<tr>
<td></td>
<td>DENVER CO 80202-3034</td>
</tr>
<tr>
<td>15. ST PAUL DIVISION</td>
<td>UNITED STATES POSTAL INSPECTION SERVICE PO BOX 64558</td>
</tr>
<tr>
<td></td>
<td>ST PAUL MN 55164-0558</td>
</tr>
<tr>
<td>16. SAN JUAN DIVISION</td>
<td>UNITED STATES POSTAL INSPECTION SERVICE PO BOX 363667</td>
</tr>
<tr>
<td></td>
<td>SAN JUAN PR 00936-3667</td>
</tr>
<tr>
<td>17. SOUTHEAST DIVISION</td>
<td>UNITED STATES POSTAL INSPECTION SERVICE PO BOX 16489</td>
</tr>
<tr>
<td></td>
<td>ATLANTA GA 30321-0489</td>
</tr>
<tr>
<td>18. SOUTHERN CALIFORNIA DIVISION</td>
<td>UNITED STATES POSTAL INSPECTION SERVICE PO BOX 2000</td>
</tr>
<tr>
<td></td>
<td>PASADENA CA 91102-2000</td>
</tr>
<tr>
<td>19. SOUTHWEST DIVISION</td>
<td>UNITED STATES POSTAL INSPECTION SERVICE PO BOX 162929</td>
</tr>
<tr>
<td></td>
<td>FT WORTH TX 76161-2929</td>
</tr>
<tr>
<td>20. TAMPA DIVISION</td>
<td>UNITED STATES POSTAL INSPECTION SERVICE PO BOX 22526</td>
</tr>
<tr>
<td></td>
<td>TAMPA FL 33622-2526</td>
</tr>
<tr>
<td>21. WASHINGTON METRO DIVISION</td>
<td>UNITED STATES POSTAL INSPECTION SERVICE PO BOX 96096</td>
</tr>
<tr>
<td></td>
<td>WASHINGTON DC 20066-6096</td>
</tr>
<tr>
<td>22. WESTERN ALLEGHENY DIVISION</td>
<td>UNITED STATES POSTAL INSPECTION SERVICE 1001 CALIFORNIA AVE</td>
</tr>
<tr>
<td></td>
<td>PITTSBURGH PA 15290-9000</td>
</tr>
<tr>
<td>23. HEADQUARTERS</td>
<td>UNITED STATES POSTAL INSPECTION SERVICE 475 L'ENFANT PLAZA SW</td>
</tr>
<tr>
<td></td>
<td>WASHINGTON DC 20260-2100</td>
</tr>
</tbody>
</table>
221.4  **Telephone Reports**

Include in any telephone report all of the following information:

a. Date and nature of occurrence.

b. Approximate loss (if none, so state).

c. Serial numbers of blank money order forms and whether issuing equipment was lost or stolen.

d. Action taken to obtain an emergency stock of items lost or stolen.

e. Address of fugitive postal offenders and aliases, if known.

f. Remedial action taken if explosive or poisonous articles are discovered or in an emergency caused by hazardous matter.

g. Notification of local police (if none, so state).

h. Security category, mailer of classified material found loose, and action taken to secure it.

221.5  **Written Reports**

Include the same information furnished by telephone and the following:

a. Serial numbers of Treasury checks lost or stolen.

b. Quantity and denominations of stamps and other accountable paper lost or stolen.

c. Amount of Postal Service funds or property lost or stolen.


e. Serial number, if any, of mail keys lost or stolen.

f. Full particulars of lost, stolen, or rifled registered mail.

g. Additional information discovered after the initial report was made.

221.6  **Nonemergencies and Routine Losses and Offenses**

Less serious losses and offenses may be reported by memorandum or by standard Postal Service forms (see Exhibit 225).

221.7  **Prohibition**

Do not discuss information about offenses or suspected offenses of postal employees with anyone outside the OIG or the Postal Inspection Service.

222  **Offenses Reported by Telephone**

222.1  **Loss or Damage**

Immediately report by telephone to the local inspector or inspector in charge any of the following losses or damages:

a. Damage to a postal unit by fire, hurricane, flood, or other catastrophe.

b. Loss of a significant amount of Postal Service funds, accountable paper, or property.
c. Loss of a rotary lock pouch, valuable registered mail, or a large quantity of other mail.

222.2 **Thefts, Burglaries, or Robberies**

Report immediately by telephone to the local inspector or inspector in charge the following thefts, burglaries (see also 227), or robberies:

a. Any employee robbed.

b. Postal unit or vehicle broken into, burglarized, or robbed.

c. Post office locks and keys (including keys and locks for mailboxes and mailbags) stolen, missing, or found under suspicious circumstances, including improper possession.

d. Indicated or suspected embezzlement. Make no further investigation or inquiry after telephone call and follow-up report.

e. Thefts, fires, and willful damage to mailboxes or contents, including customer mail receptacles, post office boxes, collection boxes, relay boxes, carrier carts and satchels, and co-op mailing racks.

f. Theft or mistreatment of mail. If a postal employee, mail contractor, or contractor employee is suspected of theft, abandonment, or other mistreatment of mail, report all known facts and make no further investigation or inquiry.

222.3 **Accidents**

Report immediately by telephone to the local inspector in charge any of the following accidents:

a. Accidents that kill or seriously injure a private person.

b. Accidents that kill or seriously injure a postal employee.

222.4 **Assaults or Threats**

Report immediately by telephone to the local inspector or inspector in charge any of the following assaults or threats (see also 223):

a. Postmaster or postal employee physically assaulted or robbed while on duty or in possession of mail, postal funds, or postal property.

b. Postal employee threatened with death or bodily injury.

c. Postal customer physically assaulted or threatened with death or bodily injury by a postal employee.

d. Libel, threats, or extortion.

e. Bomb threats.

222.5 **Controlled Substances**

If it is suspected that drugs are being used or sold on postal property or by a postal employee on duty, notify the inspector in charge immediately. Do not confront the person or make further inquiry. Hold mail suspected of containing a controlled substance and report immediately to the Postal Inspection Service.
222.6 Workers’ Compensation

Report immediately by telephone to the local inspector in charge any indicated or suspected workers’ compensation fraud or abuse relating to a postal employee. Report by telephone to the OIG (see 221.12) any information relating to suspected fraudulent claims or medical services from a health care provider (physician, clinic, hospital, pharmacy, laboratory, or other medical service person or facility).

222.61 Responsibilities

The OIG monitors and reviews the workers’ compensation program, and Postal Service efforts to combat fraudulent claims, and investigates health care providers engaged in making false claims against the Postal Service. The objective of the Postal Inspection Service is to assist injury compensation control office personnel in reducing compensation costs resulting from fraudulent claims and to gather information leading to the removal and prosecution of dishonest employees from the Postal Service.

222.62 Types of Fraud and Abuse

Some types of Federal Employees Compensation Act (FECA) fraud are noted below:

a. Concealing, with intent to defraud, prior injuries or physical impairment when hired.

b. Reporting an on-the-job injury when the injury occurred off the job.

c. Fabricating an injury or falsifying the extent or seriousness of the real injury.

d. Engaging in and concealing outside employment while receiving compensation payments.

e. Regularly engaging in activities that are inconsistent with alleged injury or medical restrictions.

f. Failing to return to work after recovering from an injury.

g. Continuing to accept compensation when no longer disabled, no longer an employee of the Postal Service, or without making any effort to return to work.

222.63 Warning Signals

To determine whether fraud or abuse exists, the employee’s supervisor should consider the following warning signals:

a. There are no witnesses to the accident (if there are witnesses, consider their reliability).

b. The injury logically cannot have happened as described.

c. The employee sustains a soft tissue versus a visible injury (e.g., no broken bones, no swelling or discoloration).

d. The injury is not reported on the day of occurrence.

e. The employee has a history of leave abuse or has previously filed questionable claims.
f. The injury is reported when disciplinary action is pending or leave of any type is denied.
g. The injury occurs shortly before an employee's defined termination date.
h. The employee is known to engage in outside activities (sports or other work) that could cause similar injury.
i. The employee has a confrontation with his or her supervisor before the accident.
j. The treating physician handles multiple claims and always indicates disability.

222.7 Stamp Offenses
Report immediately by telephone to the local inspector or inspector in charge any of the following stamp offenses:

a. Illegal use of stamps.
b. Removal of stamps from wrapper (submit wrapper or other cover with confirmation memorandum).
c. Unusual possession of stamps, which might indicate illegal use.
d. Reuse of stamps.
e. Use by postal employees in payment of debts.
f. Overcharges or undercharges of postage.
g. Alteration of meter stamps.
h. Tampering with meters.

222.8 Sabotage
Report immediately by telephone to the local inspector or inspector in charge, any indicated or suspected sabotage of mail processing equipment by a postal employee. This includes any method, procedure, or technique by which an employee is able to stop the mail processing equipment, causing downtime. Make no further investigation or inquiry.

222.9 Classified National Defense Matter

222.91 Categories
Categories of classified national defense matter are TOP SECRET, SECRET, and CONFIDENTIAL. SECRET and CONFIDENTIAL matter must be double-enveloped before entry into the mail. The outer envelope bears the address and other mailing information but no indication of the classification of the contents. The inner envelope and each page of a classified document are marked with the classification category of the contents.
222.92 Mailing Criteria

Follow these criteria for the mailing of classified matter:

a. TOP SECRET material may not be mailed but must be hand carried by courier; if any TOP SECRET material is found in the mail, it must be handled under 222.93.

b. SECRET material may be sent by registered mail.

c. CONFIDENTIAL material may be sent by certified mail.

222.93 Handling

Follow these instructions for handling classified mail:

a. Immediately give material bearing any of the classification endorsements in 222.91 and found loose in the mail by any postal employee the highest level of protection with access restricted to as few people as possible.

b. Immediately notify a postal inspector by telephone.

223 Situations Requiring Special Actions

223.1 Demonstrations, Riots, or Picketing

223.11 Immediate Notification

If demonstrations, riots, or picketing are imminent or in progress at any postal installation, immediately notify the local postal inspector or inspector in charge and the police department or other local law enforcement body.

223.12 Information Provided

Advise the local inspector or inspector in charge of the following, if known:

a. Approximate number of persons involved and cause.

b. Interference with the movement of mail.

c. Damage to postal property.

d. Blocked entrances and exits.

e. Inconvenience or criticism of customers.

f. Newspaper or other media publicity.

g. Action taken or contemplated by local, state, or federal law enforcement officials.

h. Involvement of any postal employees (if so, state whether on or off duty).

i. Involvement of any postal employee organizations.

j. Picketing (if so, state the exact messages on the picket signs).

223.13 Further Action

When individuals are not engaged in disorderly conduct, impeding postal business, or otherwise breaking local ordinances or other laws, no further action should be taken. Participants should not be permitted to remain in the
post office after normal business hours. A decision to eject participants at the conclusion of normal business hours should be cleared with the postal inspector.

223.2 Explosives

223.21 Immediate Notification

If bombs, explosives, explosive devices, or incendiary devices are discovered, report immediately to the local postal inspector. Follow cautionary steps in Publication 159-C, Contingency Planning for Bombs and Bomb Threats. Also contact the local police for assistance.

223.22 Letter or Parcel

If a letter or parcel is suspected to contain explosives, see Publication 159-C for procedures.

223.3 Counterfeit Material

223.31 Postage Stamps and Meter Indicia

If these items are presented by a customer, confiscate them and give the customer a receipt. Report by telephone to the local postal inspector and submit the postage by registered mail or hand deliver with the follow-up statement of facts.

223.32 Money Orders and Other Items

Report by telephone to the local inspector or inspector in charge any knowledge of counterfeit money orders, mail locks or keys, badges, identification cards, postmarking stamps, or postage meter impressions; and submit the counterfeit, if available, by registered mail or hand deliver.

223.4 Hazardous or Poisonous Materials

Attempt to contain and isolate the hazardous or poisonous article and evacuate the immediate area if necessary. Report immediately by telephone to the local inspector or inspector in charge if the situation presents a threat to life or property.

223.5 Suspected Narcotics

Hold mail and report immediately to the local inspector or inspector in charge, and await disposition instructions.

223.6 Express Mail Labels

Forward copies of all Express Mail labels for ZIP Codes specified by the Postal Inspection Service.
224 Offenses Reported by Memorandum

224.1 Nonmailable Matter

Report the following nonmailable matter (see also DMM C000) to the local inspector or inspector in charge by memorandum:

a. Intoxicating liquors. Withdraw from the mail and await disposition instructions.


d. Concealable firearms. Withdraw concealed firearms mailed contrary to DMM C020, pending instructions from the postal inspector in charge.

e. Matter promoting animal-fighting ventures. Submit complaints with a statement of facts.

f. Matter inciting to violence.

224.2 Lotteries

Report lotteries using the mail to the local inspector or inspector in charge. Report also any gambling or lottery operation within the post office or on postal property, except the vending or exchange of state lottery tickets at vending facilities operated by licensed blind persons, where these lotteries are authorized by state law (see DMM C030).

224.3 Procedural Irregularities

Report any of the following procedural irregularities to the local inspector or inspector in charge by memorandum:

a. COD irregularities.

b. Illegal transportation of letters in violation of the Private Express Statutes (see DMM G011).

c. Failure to pay postage, violation of franking privilege, misuse of penalty mail, depositing of advertising material in mailboxes without payment of postage, and similar schemes to evade payment of postage.

d. Delay, damage, tampering, missending, or wrong delivery of registered mail; tampering with other mail; wrong or improper delivery of other mail when financial loss or criminality is involved.

224.4 Losses

Report any of the following losses to the local inspector or inspector in charge by memorandum:

a. Losses of postal funds, accountable paper, or property not otherwise reported.

b. Loss or suspected theft of official Postal Service records known or thought to contain sensitive information.
224.5 Fraud, Forgery, Impersonation

224.51 Report any of the following acts to the local inspector or inspector in charge by memorandum:

a. Mail fraud. Request that complainant prepare a detailed statement of the facts and furnish correspondence, advertising, or other literature and envelopes in which such evidence was transmitted through the mail. Have the complainant initial and date each separate piece of evidence for future identification. Transmit this material with the report.

b. Forgery or falsification of postal records or securities, unless reported under 224.52.

c. Impersonation of a postal inspector, postal official, or other employee. Include the circumstances of the impersonation and give a complete description of the impersonator.

224.52 Report any of the following acts to the OIG by memorandum or by telephone (see 221.12):

a. Fraud against the Postal Service relating to postal contracts, including bribery, kickbacks, and conflicts of interest.

b. Fraud against the Postal Service relating to suspicious workers compensation claims from a provider.

c. Conflict of interest or misconduct involving a postal career executive service manager.

d. Impersonation of an OIG special agent or other personnel of the OIG.

225 Other Situations

Report any of the following activities to the local inspector or inspector in charge by memorandum:

a. Suspicious activities of boxholders.

b. Willful or malicious damage or injury to Postal Service property.

c. Nonpostal offenses occurring in space assigned to postal activities.

d. Money laundering offenses, including attempts to evade money order purchase reporting requirements, or use of the mails to further laundering of monetary instruments. Complete a Form 8105-A, Funds Transaction/Transfer Report, or Form 8105-B, Suspicious Transaction Report (STR), as appropriate (see 229).

e. Routine loss or offense (see Exhibit 225).
### Exhibit 225

**Reporting Routine Losses or Offenses**

<table>
<thead>
<tr>
<th>Loss or Offense</th>
<th>Action Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domestic mail — loss or rifling (including stamp stock and printed envelopes shipped by ordinary mail)</td>
<td>Submit Form 1510, Mail Loss/Rifling Report.</td>
</tr>
<tr>
<td>Military mail — loss or rifling</td>
<td>Submit Form 1510.</td>
</tr>
<tr>
<td>Parcels — rifling</td>
<td>Submit Form 673, Report of Rifled Parcel.</td>
</tr>
<tr>
<td>Customer complaints of mail theft after delivery to mail receptacles</td>
<td>Submit Form 2016, Mail Theft and Vandalism Complaint.</td>
</tr>
<tr>
<td>Theft damage (including fire) or destruction of mail receptacles and collection/relay boxes</td>
<td>Submit Form 2016.</td>
</tr>
<tr>
<td>Registered, insured, or COD mail found in supposedly empty equipment</td>
<td>Send report by letter to PO of mailing, giving full particulars, for check against index record of claims.</td>
</tr>
<tr>
<td>Canal Zone mail — mistreatment</td>
<td>See International Mail Manual (IMM) Chapter 9.</td>
</tr>
<tr>
<td>International mail — mistreatment</td>
<td>See IMM Chapter 9.</td>
</tr>
<tr>
<td>Accountability discrepancy — shortage or overage of $100 or more in official accountability of employee or contractor handling Postal Service funds or accountable paper</td>
<td>Submit Form 571, Discrepancy of $100 or More in Financial Responsibility. Show results of six previous checks of employee’s accountability. Notify inspector general if discrepancy is $100,000 or greater.</td>
</tr>
<tr>
<td>Accident claims</td>
<td>See 253.</td>
</tr>
<tr>
<td>Credit cards mailed by credit card issuer or bank</td>
<td>Submit Form 604, Credit Card Non-Receipt Report, directly to the local inspector in charge (only to be used by credit card issuer or bank).</td>
</tr>
</tbody>
</table>
Robberies

Preventive Measures

Postmasters or officers in charge are responsible for following all these preventive measures to guard against robberies:

a. Notify police and postal inspectors if suspicious strangers are observed loitering in or near the post office or following carriers on their routes.

b. Keep exterior lobby windows clear of obstruction to maximize observation of the lobby area.

c. Lock doors leading from post office box or service lobbies to workroom areas. Lock other entrances to the workroom area when not in use.

d. Lock safes, vaults, and fixed credit drawers and containers when not in use.

e. Train employees in the proper methods of activating any installed holdup alarms and cameras. Maintain and test these alarms and cameras according to instructions furnished with the equipment.

f. Discuss money or valuable mail on hand or their transportation methods only with authorized postal officials who have a need to know. Notify postal inspectors if anyone makes unusual inquiries about these items or post office security.

g. Avoid keeping excessive cash on hand. Make multiple bank deposits if large quantities of cash are received. Keep cash in employee credits and open accountability systems near the minimum amount listed in Handbook F-1, Post Office Accounting Procedures. If possible, do not count or display cash in public view.

h. Respond to an “emergency” request to open the post office only after requesting the presence of police, a postal inspector, or a postal police officer.

i. Respond to a call from the police to come to the post office after hours only after calling back and verifying the call with the police dispatcher.

j. Do not leave mail unprotected in unlocked vehicles. If the use of a satchel cart is authorized, take care to prevent thefts from the cart while delivering your route.

k. Do not make yourself or other employees attractive robbery targets. Most robbers want cash or jewelry. Often only an employee’s personal cash or property is stolen. Avoid wearing expensive jewelry and carrying more than the minimum necessary personal funds to reduce personal loss if robbed.

Actions During Robbery

The first Postal Service concern is the safety of its employees. Remain calm and try to follow these instructions:

a. Comply with the robber’s demands but give only what is demanded. If the robber presents a holdup note or other written instructions, try to
keep it for follow-up investigation by the postal inspectors and local police.

b. Do not attempt to disarm the armed robber.

c. Observe the robbers and notice details to assist in providing a description:

(1) Make comparisons between the robber and yourself or people you know to determine race, sex, age, height, weight, hair and eye color, complexion, and appearance.

(2) Remember peculiarities such as tattoos, scars, and prominent features.

(3) Remember the type and color of clothing worn (often clothing worn by a robber may be recovered and used as evidence) and whether gloves are worn.

(4) Remember the size, type, and color of weapons used, and how many of the robbers were armed.

(5) Make a mental note of everything said by the robbers, especially comments that are threatening in nature. These comments may be useful in court proceedings.

(6) Notice if the robber touches anything — the counter line, door, postal equipment, or other items.

(7) If possible without endangering your safety, observe the direction taken when the robber leaves and get the automobile description and license tag numbers. Note the color, year, make, body style, license tag number, state, and any body damage.

226.3 Actions After Robbery

226.31 Notifying Police and Inspectors

Immediately call the local police and then the postal inspectors. Give the exact location of the holdup, a description of the robbery and robbers, the license number, vehicle description, the number of occupants in the vehicle, and the direction taken upon departure. When safe to do, station someone outside to wait for the arrival of the police and postal inspectors.

226.32 Securing Building

If possible, lock all doors. Ask witnesses to remain until the local police and postal inspectors arrive. If witnesses must leave, record their full names, addresses, and home and work telephone numbers. Deny access to everyone except postal inspectors, postal police officers, the local police, and emergency medical personnel.

226.33 Protecting Evidence

Protect anything that was touched or might have been touched by the robbers. Do not touch the items yourself and prevent others from doing so.
226.34 Recording Witnesses’ Descriptions
Write down your recollection of the crime and a description of the robbers. All employees who witnessed the holdup should record their descriptions as soon as possible. For further information, consult Publication 176, Carrier Robbery/Assault, and Publication 275, Post Office Robbery.

226.35 Comparing Descriptions
Do not compare notes or recollections of the robbery with other employees or witnesses before you give your information to the postal inspectors and police.

226.36 Handling Media Inquiries
Refer all inquiries or questions about the robbery received from television, radio, or newspaper reporters to the investigating police and postal inspectors. If the police or postal inspectors authorize you to answer media inquiries, do not release the amount of robbery loss, description of items taken, or names and addresses of witnesses unless specifically authorized.

227 Burglaries

227.1 Preventive Measures
Postmasters or officers in charge are responsible for taking the following preventive measures to guard against burglaries:

a. Where possible, keep the view of building windows or entrances free from overgrown shrubbery or postal vehicles parked overnight.

b. Maintain good exterior lighting on the building and parking areas.

c. Make sure all fencing is in good condition to help prevent unauthorized persons from entering the grounds. Do not store against fences equipment that would make it easier for burglars or vandals to gain entry.

d. Secure all possible points of entry to offices, including roof openings, air conditioning vents, skylights, and roof access doors.

e. Look for such items as ladders, poles, trees, fences, dumpsters, and vehicles that a potential burglar might use to gain access to the roof.

f. Install solid core or metal exterior doors. A good solid door is a primary defense against a burglar; doors with thin wooden or glass panels do not provide adequate protection (see Handbook RE-5, Building and Site Security Requirements).

g. If exterior doors have openings of 1 square foot or more, cover the openings with bars, grating, or burglary-resistant security glass.

h. Ensure that exterior door hinges are not exposed when the doors are closed so the burglar cannot remove the hinge pins. A simple but effective means of protecting hinges on doors that open outward is to secure the hinges from the inside with a set screw.
i. Equip all exterior doors, including lookout doors and doors providing access to the workroom, with deadbolt locks, as required by Postal Service regulations.

j. If your post office has swinging vestibule doors, secure the doors with case-hardened steel chains drawn through the holes, and padlock the chains on the inside, if possible. If a Motor Vehicle Service or contract driver delivers mail after closing, the padlock must be placed on the outside. Vestibules with pedestrian doors allow chains to be padlocked on the inside.

k. Make sure that designated fire exits are not padlocked. Any device or alarm installed to restrict the improper use of egress must be designated and installed so that it cannot, even in case of failure, impede or prevent emergency egress. Consult the National Fire Protection Association (NFPA) Life Safety Code requirements or your safety officer for proper use of locks on exterior doors.

l. Make sure that keys for retail cabinets or alarm controls are not left in desk drawers or anywhere else a burglar can find them. Issue Postal Service keys to employees only when necessary. Issue building keys only to employees required to open the office in the morning or close the office at night.

m. Protect windows with grating or wire mesh grills if the windows are less than 10 feet from the ground and are not visible from the street or are in an office susceptible to attack. Install interior locks on operable windows.

n. Protect parcel drops. Barrel-type parcel drops provide the best defense against unauthorized entry. Steel cages can be built around the inside of the parcel drops, if necessary, to prevent entry by juveniles.

o. If the post office is equipped with an alarm system, make sure it is operational. Periodically check alarm system batteries and replace any that are leaking or corroded. Keep alarm functions and sensor locations on a need-to-know basis and report any alarm malfunctions to the inspector in charge.

p. Give postal funds maximum protection. Place cash, food coupons, stamp stock, and money order forms in security containers, vaults, burglar resistant chests, or fireproof safes.

q. If possible, detach wheels from safes so that they cannot be easily removed from the post office.

r. Be sure safes and vaults are fully locked at the end of the day. Give the dial at least two complete turns in each direction.

s. Do not hide the combination to the safe anywhere in the office such as on calendars or in desk drawers. Only authorized postal employees on a need-to-know basis should have the combination of any security container or safe used to protect postal funds.

t. Do not leave large amounts of cash in the office overnight. Deposit surplus funds in the bank or prepare a dispatch of the bank deposits as required by current instructions.
227.2 **Actions After Burglary**

227.21 **Before Entry**
If arriving at work and discovering the post office has been burglarized, follow these instructions:

a. Stay outside the building.

b. Telephone local police and postal inspectors immediately.

c. Stay a safe distance away and observe entry points.

d. Observe and write down any descriptions, license numbers, or other information.

e. Wait for police and postal inspectors to arrive.

227.22 **After Entry**
If a burglary is not obvious until after entering the post office, follow these instructions:

a. Telephone local police and postal inspectors immediately.

b. Protect the crime scene.

c. Lock doors.

d. Touch nothing and keep others away from the area.

---

228 **Assaults**

228.1 **Employees and Customers**

228.11 **Postal Inspection Service Investigations**
The Postal Inspection Service investigates employment-related assaults and threats against employees and customers occurring on postal premises or committed by employees while on duty or because of official employment.

228.12 **Prosecution of Assailants**
Assault on a postal employee engaged in the performance of official duties or because of the performance of official duties may result in prosecution of the assailant under federal or state and local laws.

228.13 **Disciplinary Action of Employees**
Employees assaulting or threatening other employees or postal customers may be subject to remedial or disciplinary action, including discharge and prosecution under federal, state, or local laws.

228.2 **Reporting Assaults**
Call local police and the inspector in charge or local inspector when an employee or customer is physically assaulted or threatened with death or bodily harm. Follow the telephone report to the Postal Inspection Service by a memo or other written report.
Money Laundering and Foreign Asset Controls

Money Laundering Control

Policy

Postal Service policy is to follow both the letter and the spirit of the law and the regulations pertaining to the Money Laundering Control Act and those portions of title 31 of the United States Code (U.S.C.) referred to as the Bank Secrecy Act (BSA). The Postal Service is committed to minimizing the use of postal money orders, wire transfers, and stored value cards in illegal money laundering schemes. The Secretary of the Treasury delegates to the Postal Service the power to implement, monitor, and enforce its own compliance program under 31 U.S.C. 5318(a)(1).

Responsibilities

Compliance Officer

The Postal Service compliance officer is responsible for creating, implementing, maintaining, and monitoring the Postal Service’s compliance program. This responsibility includes the following:

a. Ensuring that postal and contract employees adhere to all aspects of the Bank Secrecy Act.

b. Implementing and maintaining a national BSA training program.

c. Ensuring that adequate internal controls and procedures are in place to assist employees in complying with the standard and suspicious transaction reporting requirements of the law and to detect noncompliance by postal and contract employees.

d. Referring instances of noncompliance to the appropriate postal manager or supervisor or to the Postal Inspection Service or the OIG for appropriate action.

e. Reporting instances of postal and contract employee noncompliance and instances of suspicious activity by postal customers to the Department of the Treasury in such format and time frame as the Secretary of the Treasury prescribes.

Postal and Contract Employees

Postal and contract employees are responsible for complying with all recording and reporting requirements of the Bank Secrecy Act. This responsibility includes:

a. When selling wire transfers and stored value cards for cash equal to or greater than $1,000 and less than $3,000 in any combination to the same customer in the same day, completing Form 8105-A, Funds Transaction/Transfer Report, with the following information:

   (1) Purchaser’s name.
   (2) Purchaser’s address.
   (3) Purchaser’s photo identification number.
   (4) Type of photo identification if other than a driver’s license.
(5) Date of purchase.
(6) Dollar amount of purchase.
(7) Recipient’s name (for wire transfers).
(8) Recipient’s address (for wire transfers).
(9) Transaction number of wire transfer(s) and/or item number of stored value cards purchased.

b. When selling money orders, wire transfers, and stored value cards for cash equal to or greater than $3,000 in any combination to the same customer in the same day, completing Form 8105-A with the following information:
(1) Items (1) through (8) above.
(2) Purchaser’s Social Security number (or alien registration or passport number).
(3) Purchaser’s date of birth.
(4) Inclusive serial numbers of money orders purchased, transaction number or wire transfer(s), and/or item number of stored value cards purchased.

c. Completing a Form 8105-B, Suspicious Transaction Report (STR), for any cash transaction deemed suspicious by the employee, regardless of the dollar amount or type of transaction. Suspicious activity might include frequent and large cash purchases of money orders, wire transfers, or stored value cards or paying for services, such as meter settings and trust funds, with cash rather than company checks.

d. Never advising customers how to structure purchases in order to avoid having to provide identifying information (photo ID, Social Security number, etc.).

e. Never selling money orders, wire transfers, and stored value cards for cash totaling $10,000 or more in any combination to the same customer in the same day, even if the employee completes Form 8105-A for the transaction(s).

f. Never cashing money orders or paying out wire transfers totaling $10,000 or more in any combination to the same customer in the same day, even if the employee completes Form 8105-A for the transaction(s).

229.123 Office of Inspector General and Postal Inspection Service

The OIG conducts audits of the Postal Service’s compliance with the Bank Secrecy Act. The OIG and the Postal Inspection Service investigate, as appropriate, the use of postal products and services in criminal activities. This may include analyzing Forms 8105-A, Forms 8105-B, and suspicious money order, wire transfer, and stored value card sales and redemptions to detect possible criminal activity.
229.13 *Training*

All postal and contract employees, including postmasters and supervisors, assigned to retail sales positions participate in a formal training program that includes instruction on:

b. Standard reporting using Form 8105-A.
c. Detection of suspicious transactions.
d. Suspicious transaction reporting using Form 8105-B.

229.14 *Internal Controls*

Supervisors have the following responsibilities:

a. Ensuring that established internal controls and procedures are in place at their respective units.
b. Taking immediate corrective action when notified by the Postal Service BSA compliance officer that an employee has not followed any one of the procedures listed in 229.122.
c. Documenting corrective action taken when incidences of noncompliance are detected.

229.2 *Foreign Asset Control*

229.21 *Policy*

Postal Service policy is to follow both the letter and the spirit of the law and the regulations dealing with economic sanctions that the U.S. government imposes against certain foreign countries, foreign nationals, and specially designated nations. The Postal Service is committed to ensuring that direct service international money orders and wire transfers are not used to violate these laws and regulations. These laws and regulations are found in the following:


229.22 *Compliance Officer Responsibilities*

The Postal Service compliance officer is responsible for creating, implementing, maintaining, and monitoring the Postal Service’s compliance with the laws and regulations in coordination with the Office of Foreign Asset Control, Department of the Treasury. This responsibility includes the following:

a. Ensuring that postal management adheres to all aspects of the laws, including implementing and maintaining program filters for direct service international money order financial transactions and wire
transfers, and that adequate internal controls and procedures are in place to ensure compliance by postal and contract employees.

b. Reporting instances of the freezing of assets to the Office of Foreign Asset Control, Department of the Treasury, in such format and time frame as the Secretary of the Treasury prescribes.

23 Withdrawal of Mail Privileges

231 False Representation and Lottery Orders

231.1 Issuance

By law (39 U.S.C. 3005), acting on satisfactory evidence, the judicial officer may issue a mail-stop order against anyone seeking mailed remittance of money or property by means of a false representation or lottery scheme. These orders provide for return of the mail and refund to senders of postal money orders.

231.2 Enforcement

Notice of these orders is published in the Postal Bulletin. Generally, an order against a domestic enterprise is enforced only by the post office designated in the order. All facilities processing mail for dispatch abroad assist in enforcing orders against foreign enterprises by forwarding mail addressed to these enterprises to designated post offices.

232 Fictitious Name or Address Orders

232.1 Issuance

By law (39 U.S.C. 3003 and 3004), when satisfactory evidence exists that mail is addressed to a fictitious name, title, or address used for any unlawful business and no one has established a right to have the mail delivered; or mail is addressed to places other than the residence or regular business address of the addressee to enable the addressee to escape identification, then the judicial officer may, under 39 CFR 964, order the mail returned to the sender.

232.2 Enforcement

24 Audits

241 Responsibility

241.1 Inspector General

The inspector general is responsible for independently assessing the programs and operations of the Postal Service and apprising the Governors and Congress of significant observations. The inspector general directs the development of policies, plans, and procedures governing all audits, evaluations, and inspections. These activities are performed by the OIG, the Postal Inspection Service, and independent certified public accountants, as authorized.

241.2 Role and Function

Independent OIG and Postal Inspection Service audits and other reviews play important roles as management tools for evaluating whether operations are executed economically, efficiently, and effectively. OIG and Postal Inspection Service personnel do not exercise authority over persons in the organizations reviewed. Findings and observations are provided to make management aware of any problems noted during a review. Recommendations and suggestions are offered as workable solutions to noted problems. However, management cannot, and should not, completely rely on auditors, evaluators and/or inspectors to detect problems and recommend solutions. Managers must routinely assess their own operations to assure themselves and their superiors that operations are well controlled and meet the goals and objectives of the organization. Management is responsible to promptly and properly initiate corrective action, if auditors, evaluators, inspectors, or managers find problems.

242 Background

242.1 Authority

The Inspector General Act of 1978, amended in September 1996 (Public Law 104-208), created an independent Office of Inspector General (OIG) for the Postal Service (5 U.S.C. App. 3). The inspector general has delegated authority to the Postal Inspection Service to perform selected audit activities in coordination with the OIG. This coordinated audit program ensures the optimum use of resources and provides independent examinations and evaluations of postal activities at all levels of the organization without duplication of effort.

242.2 Standards

OIG and Postal Inspection Service work complies with appropriate standards established by the comptroller general of the United States, the President's Council on Integrity and Efficiency, the American Institute of Certified Public Accountants, and the Institute of Internal Auditors.
243 **Mission**

243.1 **Objective**

OIG and Postal Inspection Service work is performed to:

a. Provide an independent check on the adequacy and effectiveness of systems of control to ensure achievement of corporate goals.

b. Determine compliance with Postal Service policies and procedures and public laws.

c. Verify the existence of assets and assure that proper safeguards are maintained to detect failures that may lead to fraud, waste, and abuse.

d. Assess the reliability and operation of accounting and reporting systems.

e. Review operations for economy and efficiency, and effective use of resources.

f. Evaluate the effectiveness of management’s corrective actions relating to identified problems and deficiencies.

243.2 **Project Category Overview**

a. *Performance* — The OIG is responsible for conducting all postal-wide performance audits. The OIG also conducts audits and evaluations at other levels to test systems and/or internal controls. The Postal Inspection Service is responsible for conducting installation, district, and area performance audits and reviews of the Postal Service.

b. *Financial* — The OIG directs all financial audit opinion activity, and conducts other financially related audits. The Postal Inspection Service is responsible for conducting installation and district financial audits of the Postal Service.

c. *Contract* — Contract audits performed by the OIG address systemic issues within the purchasing process, and significant individual procurements. The Postal Inspection Service is responsible for conducting pre- and post-award contract audits, requested by contracting officials. The OIG analyzes results of all contract audit work to identify trends, patterns, and issues relating to postal contractors and contract administration.

d. *Developmental* — Developmental audit work is performed by the OIG and is intended to provide management with an assessment of the design and integrity of internal controls during the early phases of new projects. These projects include automation, technical, information-based, and business process projects. Developmental work encompasses both performance and financial auditing issues, with an emphasis on an independent assessment and evaluation of new or redesigned systems.

e. *Consulting services* — Management may request consulting services from the OIG, which are distinct from the usual audits, evaluations, and inspections. The OIG can provide assistance in areas such as process improvement projects; facilitating self-assessments outside of
“traditional” internal control activities, training, and studies relating to implementation of audit report recommendations.

243.3 **Process Overview**

OIG and Postal Inspection Service projects generally adhere to the following process:

a. Announcement letters are issued at the start of a project to solicit management’s input and perspective.

b. Entrance conferences ensure that management is provided an opportunity to discuss the project scope and objectives.

c. Surveys are conducted to formulate specific project objectives and determine the scope of the project.

d. Field work and data analysis is performed to independently assess the programs/operations within the scope of the project.

e. Draft reports or memoranda are issued to management to communicate the results of observations and analyses.

f. Exit conferences and working meetings ensure that management is aware of pertinent issues and provides a forum for discussion.

g. Management responses are requested, evaluated, and included in the final report.

h. Final reports are distributed to appropriate levels of management to ensure that issues are adequately addressed.

243.4 **Cooperation**

Postal officials and employees must extend maximum assistance to auditors, evaluators, inspectors, and authorized representatives of the OIG and Postal Inspection Service to ensure audit objectives are achieved.

243.5 **Liaison**

Outside organizations such as the General Accounting Office and the independent certified public accountants hired by the Board of Governors also provide selective reviews of Postal Service activities. The OIG maintains liaison and coordinates activities with these and other external organizations providing audit attention.

244 **Reports**

244.1 **Definitions**

244.11 **Audit Reports**

Audit reports communicate audit findings, conclusions, and recommendations to management. Responsible managers must respond to all recommendations made in these reports. When a response is requested via transmittal letter (see 244.13), it is Postal Service policy to prepare a written response.
244.12 Other Reports
Other reports and memoranda communicate observations, conclusions and suggestions to management. Each manager is given an opportunity to respond to the suggestions contained in the reports and memoranda. Written responses are required when appropriate.

244.13 Transmittal Letters
Each report is distributed with a transmittal letter offering to hold an exit conference and requesting a written response within a specified time frame. Management is required to respond to reports by addressing each finding, recommendation, and identified savings as detailed in 244.14.

244.14 Management Responses
Management’s response to audit reports, and other reports when requested, should include the following:

a. Whether the official agrees with each finding or observation.
b. Whether the official agrees with each recommendation/suggestion.
c. Whether the official agrees to any identified savings.
d. What specifically will be done, including an evaluation of any special assistance needed in carrying out the recommendation.
e. Who in the organization will take the corrective action.
f. A timeline for completion and when the corrective action will be implemented. If implementation is deferred beyond 12 months, include the reason for delay.

Management responses to the draft report are evaluated and incorporated into the final report in synopsis form. A verbatim copy of the response may be included in the final report. The final report is then transmitted to the responsible managers, under the signature of the appropriate OIG or Postal Inspection Service issuing authority.

244.2 Release and Distribution of Audit Reports

244.21 Headquarters

244.211 Office of Inspector General
The inspector general or appropriate assistant inspector general transmits reports of Headquarters interest and those reports containing recommendations for Headquarters action to the appropriate Headquarters unit.

244.212 Postal Inspection Service
When installation, district or area level audits identify issues requiring Headquarters action, the inspectors forward the issue through the deputy chief inspector Business Investigations to the assistant inspector general for Performance (Audit). The appropriate assistant inspector general reviews the issue and, in coordination with the deputy chief inspector Business Investigations, determines the appropriate course of action. The deputy chief inspector notifies inspectors of the final disposition.
244.213 **Audit Control Coordinator**

The audit control coordinator reports to the controller and serves as a focal point for all postal audit activity. The OIG will provide copies of all reports transmitted to Headquarters officials to the audit control coordinator. Headquarters officials with an interest in any audited activity or function may request copies of reports from the coordinator.

244.22 **Levels Below Headquarters**

244.221 **Performance Audits**

When audit reports include recommendations to area office management or other levels below Headquarters, a draft report is submitted to the manager of the installation or activity audited. Draft reports issued by the OIG are transmitted to the responsible postal manager under the signature of the appropriate assistant inspector general. For audit activities performed by the Postal Inspection Service, draft reports are transmitted to the responsible postal manager under signature of the inspector in charge of the project leader performing the work. Management responses to draft performance audit recommendations must be incorporated into the final report at the project leader level. The final report is then submitted to the responsible postal official under the signature of the appropriate assistant inspector general or inspector in charge.

244.222 **Financial Audits**

At the conclusion of financial audits of post offices and facilities findings and recommendations will be discussed with the facility head during an exit conference. The manager reviews the report and replies (if requested by the project leader) within the specified time frame. The comments are then included in the final report, which is sent to the responsible postal official and the next higher level of management.

244.223 **Contract Audits**

OIG contract audit reports include findings and recommendations for corrective actions by management officials. These types of audit reports will be handled in accordance with the policies previously set forth in 244.211 and 244.221. Contract audit reports issued by the Postal Inspection Service provide an opinion on the adequacy of cost or pricing data submitted by postal contractors. These reports are advisory in nature and are issued in final form directly to the requesting official.

244.224 **Distribution of Report Copies**

A copy of each final report transmitted by the OIG will be forwarded to the assistant inspector general for Performance (Audit) and the audit control coordinator. A copy of each final report transmitted by the Postal Inspection Service will be forwarded through the deputy chief inspector to the assistant inspector general for Performance (Audit) and the audit control coordinator. The Postal Inspection Service will provide to the OIG post negotiation memorandums and any other documentation showing the disposition of reported audit findings for the contract audits it performs.
Implementation of Audit Recommendations

245.1 Management Responsibility
Management must ensure the implementation of audit recommendations to which they have agreed.

245.2 Audit Follow-Up

245.21 Status
The audit control coordinator is responsible for maintaining management’s audit tracking and reporting system. Periodic status updates on the implementation of management action on recommendations/suggestions will be provided to management, the Postal Inspection Service and the OIG, as appropriate. This follow-up process is required by the inspector general legislation and OMB Circular A-50. The appropriate Headquarters, area, or district office responsible for the implementation of corrective action must identify any formalized plan to respond to audit recommendations, and periodically report the current status to the audit control coordinator, as requested.

245.22 Periodic Reviews
The OIG or the Postal Inspection Service, as appropriate, will conduct periodic follow-up reviews to assess the effectiveness of management’s actions.

245.3 Coordinating, Tracking, and Reporting

245.31 Headquarters Level

245.311 Deputy Postmaster General
The deputy postmaster general has overall responsibility for the implementation of audit recommendations made to groups for which the deputy postmaster general is responsible. In addition, the deputy postmaster general also is responsible for reviews of those groups answering to the postmaster general. The audit control coordinator reviews implementation of recommendations or suggestions and generates exception reports for the deputy postmaster general. The audit control coordinator prepares a report on the status of each recommendation for inclusion with the semi-annual report to Congress.

245.312 Vice Presidents
Each vice president designates a person responsible for tracking the implementation of audit recommendations within that unit. The vice president’s designee provides the chief operating officer with the results of the audit control coordinator status requests.

245.313 Units Reporting to Postmaster General
Each vice president who reports to the postmaster general designates a person for tracking the implementation of audit recommendations within that
245.314 Audits and Investigations

unit. The designee furnishes the results of status requests to the audit control coordinator, with a copy to the deputy postmaster general.

245.314 Schedule

Vice presidents ensure that audit recommendations are carried out as soon as practical. They must establish a target date for full implementation and monitor follow-up action. They must document the status of implementation for subsequent review by the audit control coordinator, the Postal Inspection Service, and the OIG.

245.32 Area Office Level

Each vice president of Area Operations is responsible for overall control of the follow-up on implementing audit recommendations within the area office. Each vice president of Area Operations designates a position responsible for reviewing the results of audit control coordinator status requests on the implementation of audit recommendations directed to the area office, plant, and district levels. The vice president of Area Operations’ designee evaluates the action taken by field managers to ensure implementation of audit recommendations and personally advises the vice president of Area Operations of the results and furnishes the results of status requests to the audit control coordinator.

245.33 District Level

245.331 Review

District managers review each audit report on facilities within their jurisdictions. They provide a written response within the specified time frame when requested by the OIG or the Postal Inspection Service. They monitor the implementation of recommendations at facilities reporting to the district. They review audit control coordinator status request reports from the installation head of the audited facility to ensure that action is taken to implement audit recommendations. They also ascertain that corresponding service and budget objectives are achieved. The final status report submitted must clearly show that audit recommendations are implemented and reported savings realized.

245.332 Reporting

District managers report to the vice president of Area Operations on audit control coordinator status requests for the steps taken to carry out the recommendations or the reasons for delay in implementation.

246 Application of Audit Findings

246.1 Vice President, Area Operations

The vice president of Area Operations’ designee reviews audit reports bearing on matters within the area and annually summarizes significant findings and recommendations for distribution to all district managers within the area office.
246.2 District Manager
District managers review the summary and determine whether the findings
and recommendations apply to their offices. Distribution of the summary is
made to all managers within their districts.

246.3 Field Manager

246.31 Review
Field managers review the summary and determine whether the findings and
recommendations apply to their offices.

246.32 Report
Within 30 days after receipt of the summary, each field manager reports the
results of the self-review to the appropriate district manager. Where similar
conditions are found to exist, the date corrective action was taken or is
estimated to begin is included in the report. Document improvements in
service or reductions in cost.

246.33 Implementation
When implementation depends on the occurrence, such as training or
acquisition of equipment, field managers must include target dates for each
step of the implementation.

247 Requests for Audit Attention

247.1 Headquarters Level
All requests for audit attention generated from the postmaster general,
deputy postmaster general, vice presidents, or other headquarters personnel
are directed to the inspector general, with a copy to the audit control
coordinator.

247.2 Area Level
Requests for audit attention generated from vice presidents of Area
Operations or other area personnel, including installation and district
compliance audits within the area are directed to the appropriate inspector in
charge, with a copy to the audit control coordinator. Where concerns or
issues arise from policies or processes issued postal-wide from
headquarters, requests from area personnel are directed to the inspector
general, with a copy to the audit control coordinator.

247.3 District Level
Requests for audit attention generated from district managers or other district
personnel are directed to the local inspector in charge, with a copy to the
audit control coordinator.
247.4 Field Level

Requests for audit attention generated from field managers or installation heads are directed to the local inspector in charge, with a copy to the audit control coordinator.

25 Tort Claims

251 Responsibilities

251.1 Postal Service

251.11 Definition

Tort claims are claims for damage to or loss of property, personal injury, or death caused by the negligent or wrongful act or omission of an employee while acting within the scope of employment.

251.12 Authority

The Postal Service is authorized to settle claims under the Federal Tort Claims Act.

251.13 Policy

Postal Service policy is to promptly and willingly discharge its legal responsibility to those persons who claim damages pursuant to the Federal Tort Claims Act.

251.2 General Services Administration (GSA)

GSA investigates and settles tort claims for damages from accidents at facilities under GSA control.

252 Accident Investigation

252.1 Accidents to Be Investigated

Investigate both vehicular and nonvehicular accidents of all types involving personal injury or property damage to private persons where the Postal Service or an employee is involved, except OIG personnel. Investigation of accidents involving OIG employees should be referred to the OIG for internal investigation.

252.2 Responsibility

252.21 Reference

Detailed instructions are in Handbook PO-702, Accident Investigations — Tort Claims.
252.22 Installation Head or Designee

252.221 On-the-Scene Investigations
Conduct prompt on-the-scene investigations of all accidents involving damage to private property or personal injury to private persons following Handbook PO-702.

252.222 Personal Injury and Private Property
When personal injury is involved or when damage to private property is estimated to exceed $1,000, notify the accident investigator before or immediately after returning from the accident scene. Further investigation is based on the advice of the accident investigator.

252.23 Accident Investigator

252.231 Selection
The district Customer Support Services manager designates in writing an accident investigator. Where vehicle operations supervisory personnel are assigned, select from these employees. Otherwise, designate a responsible supervisor, preferably a delivery services supervisor. The accident investigator selected should be a person who makes independent, sound judgments and communicates effectively. The individual assigned must be trained as an accident investigator.

252.232 Duties
The accident investigator has the following responsibilities:

a. Conducts both on-the-scene and follow-up investigations of all accidents within the city where the installation is located involving damage to private property or personal injury to private parties.

b. Serves as a consultant and adviser to associate office personnel designated under 252.221 to investigate accidents.

c. Trains post office personnel and ensures their accident investigation proficiency.

d. Makes sure that all information, exhibits, and documentation about accidents involving personal injury to private persons or damage to private property in excess of $1,000 are forwarded promptly for evaluation.

e. When a claim is received, determines if any necessary follow-up action is required.

f. Forwards the completed investigative file promptly to the adjudicating authority (see 254).

g. Decides whether personal assistance is necessary at the scene or if guidance to the local investigator suffices when notified of the accident.

h. Promptly contacts the chief field counsel on learning of an accident involving Postal Inspection Service employees (see 254.1).

i. Promptly contacts the general counsel for the inspector general on learning of an accident involving OIG employees.
252.24 Accident Investigator and Claims Coordinator
The accident investigator and claims coordinator (occupational code 0992-5002) plays an important role in accident investigations and tort claims processing.

252.3 Scope of Investigations
Promptly obtain full information and facts about responsibility for the accident and the character and extent of any damage sustained. Make thorough and complete inspections and reports of personal injury cases and accidents resulting in property damage. Supplement the report of a postal employee involved in either type of accident with written statements or affidavits from witnesses and from the parties injured or whose property was damaged.

252.4 Verification of Damages
Have a body and fender repairman in the motor vehicle service or some other qualified employee carefully check for accuracy all bills submitted by claimants for damages to property. Ensure that all items included in a claim are for repairs of damage actually caused by the specific accident.

253 Preparing Reports and Claims

253.1 Postal Official in Charge

253.11 General Instructions
Attach all required forms when submitting a report of an accident. Keep a complete file (copies of all forms) in the installation files.

253.12 Forms Required

253.121 Form 2198
Submit the requested information on Form 2198, Accident Report — Tort Claim, with particular emphasis on your opinion about the negligence of the postal employee involved, whether the bills or estimates supporting the claim are accurate and represent a reasonable charge for the damage involved, and recommendation for action to be taken.

253.122 Standard Form 91
SF 91, Operator's Report of Motor Vehicle Accident, is carried in each government motor vehicle, privately owned government-operated motor vehicle, and by each employee using a bicycle or light vehicle. The form is filled out by the driver of any vehicle involved in an accident, regardless of the extent of injury or damage, and whether the parties involved state that no claim is to be filed. Vehicle operators must not give any statements, written or oral, at the scene of the accident, except information required by law to be furnished to other drivers or parties involved.

253.123 Form 1700
Form 1700, Accident Investigation Worksheet, must be completed for both vehicle and nonvehicle accidents.
253.224 **Standard Form 94**
Standard Form 94, *Statement of Witness*, is filled out by all available witnesses to an accident. Instruct vehicle operators and other employees to obtain the names and addresses of any persons who may have witnessed the accident. The claimant does not have to fill out this form.

253.2 **Claims Procedures**

253.21 **General**

253.211 **Assistance**
Any person who indicates a desire to file a claim should be given a full explanation of claims procedures and an SF 95, *Claim for Damage, Injury, or Death*. When necessary, desirable, and considered in the best interest of the Postal Service, the person should receive help to prepare the form and assemble evidence.

253.212 **Restrictions**
Postal Service employees are prohibited from:

a. Receiving any gratuity for services.

b. Accepting any interest in a claim.

c. Disclosing information that may be made the basis of a claim, any evidence, or any record in any claim matter unless provided by law.

253.22 **Administrative Claims**

253.221 **Definition**
An *administrative claim* is a properly completed SF 95 or any other written notification received from a claimant, a duly authorized agent, or legal representative, accompanied by any claim for money damages in a specified sum (*sum certain*) for injury to or loss of property, personal injury, or death alleged to have occurred by reason of the incident. An administrative claim is not required to be filed on an SF 95, but the claimant should file the claim on this form when possible.

253.222 **Insurance Information**
Every claimant must state in writing, as part of a claim for property damage:

a. Whether collision insurance is carried and, if so, the name and address of the insurance company, policy number, and type of coverage (full or deductible).

b. Whether a claim is filed with the insurance company.

c. If a claim is filed, the action the insurer has taken or proposes to take with reference to the claim.

d. Whether public liability and property damage coverage is carried by the claimant, and if so, the name of the insurance carrier.
253.223 **Who May File**

Claims may be filed as follows:

a. A claim for injury to or loss of property may be presented by the owner of the property or his or her duly authorized agent or legal representative.

b. A claim for personal injury may be presented by the injured person or his or her duly authorized agent or legal representative.

c. A claim based on death may be presented by the executor or administrator of the decedent’s estate or by any other person legally entitled to assert such a claim under applicable state law.

d. A claim for loss wholly compensated by an insurer with the rights of a subrogee may be presented by the insurer. A claim for loss partially compensated by an insurer with the rights of a subrogee may be presented by the parties individually as their respective interests appear or jointly (see also 253.24).

e. A claim signed by an agent or legal representative on behalf of a claimant is presented in the name of the claimant; it must show title or legal capacity of the person signing and be accompanied by evidence of authority to present a claim on behalf of the claimant as agent, executor, administrator, parent, guardian, or other representative.

253.23 **Processing Administrative Claims**

253.231 **General Instructions**

Stamp or write the date and sign the original and copies of any claim forms *immediately on receipt*. Do not return any forms or papers received from a claimant or representative. Copies may be provided.

253.232 **Incomplete or Indefinite Claims**

Handle an incomplete or indefinite form as follows:

a. Note that a claim is incomplete or indefinite if it does not provide all necessary information, as in any of the following cases:
   
   (1) It lacks the answers to the questions on insurance as required by 253.222.
   
   (2) It does not contain a demand in a specific amount.
   
   (3) It is not properly signed.
   
   (4) It is deficient in some other way.

b. On receipt of an incomplete or indefinite claim, furnish the claimant or representative a blank SF 95 and request that it be filled out completely.

c. If a claim is not filed on an SF 95, but is a claim as defined in 253.221, furnish the claimant an SF 95 and request that it be filled out completely.

d. If a reply to a request to complete an SF 95 is not received within 15 days, do not hold the investigative file, but forward it as directed in 254.3.
e. If a reply is received that resolves the deficiency by a document other than SF 95, do not insist on the completion of an SF 95. Forward the investigative file as soon as possible as directed in 254.3.

253.24 **Claims by Insurance Companies (Subrogation)**

Insurers (subrogees) presenting a claim in their own name or with their insured (subrogor) must state their interest or right to file a claim by appropriate documentary evidence such as a Form 2188, *Subrogation Receipt*, a Proof of Loss statement, or other such form signed by the insured and including words of subrogation. A copy of the insurer’s check evidencing payment to or on behalf of the insured is appropriate evidence of the insurer’s right to make a claim.

254 **Processing Reports and Claims**

254.1 **Serious Accidents**

254.11 **Definition**

An accident is considered a *serious accident* if:

a. Civil or criminal action is brought against a postal employee involved in an accident.

b. Injury to private individuals results in any of the following:
   
   (1) Death.
   
   (2) Dismemberment.
   
   (3) Total or partial loss of vision.
   
   (4) A medical prognosis of extensive hospitalization or prolonged disability.
   
   (5) Damage to private property estimated to exceed $25,000.

254.12 **Immediate Notice**

Immediately notify the chief field counsel when a serious accident occurs.

254.13 **Complete Report Required**

This preliminary report is not a substitute for a complete investigation and the preparation of other required reports.

254.2 **Claims Payment Authority**

254.21 **Personal Injury and Property Damage Claims of $1,000 or Less**

When the amount of claim is $1,000 or less, the district manager, postmaster, or designee is authorized, except as noted in 254.22, to pay (but not to deny) the claim after determining that the damage claimed was caused by the negligent or wrongful act or omission of a postal employee while acting in the scope of employment. This delegation of authority is limited to the payment of claims made by the public for damages arising out of incidents such as a motor vehicle accident, a slip, trip, or fall accident, or similar occurrence.
254.22 **Claims Payment Unauthorized**
The district manager or postmaster may not pay any of the following:

a. Any claim arising out of the loss, miscarriage, or negligent transmission of letters or postal matter.

b. Any claim arising out of assault, battery, false imprisonment, false arrest, malicious prosecution, abuse of process, libel, slander, misrepresentation, deceit, or interference with contract rights.

c. Any claim submitted by a federal agency.

d. Any claim submitted by a federal employee.

e. Any claim arising out of an accident in which the postal employee involved received workers’ compensation or continuation of pay.

254.23 **Denied Claims**
The above listed claims and all tort claims that are recommended for denial must be forwarded to the chief field counsel’s office or the Information Systems Service Center, as explained in 254.31, 254.32, and 254.33.

254.24 **Multiple Claims**
If more than one claim arises or may arise out of a single accident, the district manager or postmaster may pay each claim presented, if none of the claims or anticipated claims exceeds the delegated authority of $1,000.

254.25 **Claim Payment**
Payment of claims by the district manager or postmaster must be entered to AIC 597, Tort Claims — $5000 or Less (District Offices only), in the accountbook. A summary report, together with all supporting documents and exhibits, should be retained to support the accountbook entry (see Handbook PO-702, *Accident Investigation — Tort Claims*).

254.26 **Advising Claimants**
Before paying a claim under 254.31, 254.32, and 254.33, do not advise a claimant or a claimant’s representative that the Postal Service accepts liability or plans to pay for any expenses incurred such as rental of a replacement vehicle.

254.3 **Processing Claims**

254.31 **Property Damage Claims Over $5,000**
When the claim of one individual, including a claim of an insurance company, is more than $5,000, submit reports and forms immediately to the chief field counsel.
254.32 **Personal Injury Claims Over $1,000**
When the amount of the personal injury claim of an individual is more than $1,000, submit reports and forms immediately to the chief field counsel.

254.33 **Property Damage Claims, $1,000 to $5,000**
When the amount of the property damage claim of an individual is $1,000 to $5,000, including a claim of an insurance company, submit reports and forms to:
SAN MATEO ACCOUNTING SERVICE CENTER
UNITED STATES POSTAL SERVICE
2700 CAMPUS DR
SAN MATEO CA 94497-9400

254.34 **Narrative Report**
A narrative report, as described in Handbook PO-702, *Accident Investigation — Tort Claims*, must be included when submitting a claim to the chief field counsel.

254.35 **Multiple Claims**
When claims from one accident are received from several claimants, and any one of the claims received or anticipated is for more than $1,000, forward all reports and related forms under 254.31, 254.32, and 254.33.

254.36 **Accidents With No Claim Received**
Do not forward any accident files before a claim is received.

254.37 **Denial of Claims**
The district manager or postmaster may not deny any tort claim.

254.38 **Assistance**
Contact the San Mateo Accounting Service Center, Postal Inspection Service accident consultant, or chief field counsel for any assistance needed.

254.4 **Reports to GSA**

254.41 **Accidents Involving GSA-Controlled Buildings**
Do not investigate accidents occurring in post offices quartered in a federal building owned, operated, and maintained by GSA. Advise the GSA building manager or other GSA official of the accident.

254.42 **Accidents Involving GSA Vehicles**
If a postal employee is involved in an accident while operating a GSA vehicle, the initial investigation is conducted as required by 252.

254.5 **Accidents in Leased Quarters**
Investigate all accidents involving private persons that occur in leased or rented facilities just as fully as those occurring on postal-owned premises. In accidents caused or alleged to be the result of structural defect, state if,
when, and how notice of the defect and needed repairs was given by the Postal Service to the landlord before the accident occurred. Advise if lease contains a provision requiring the landlord to make repairs. Include a copy of the lease and all available information on the landlord’s insurance coverage.

26 (Reserved)

27 Security

271 General Responsibilities

271.1 Chief Inspector

The chief inspector is designated as the security officer for the Postal Service. This official issues instructions and regulations on security requirements. Authority for implementation and management of a data security processing program is delegated to the vice president of Information Systems. Authority for directing and administering the internal security program for the OIG is delegated to the inspector general.

271.2 Installation Heads

Installation heads are responsible for ensuring the safety of on-duty postal employees, as well as the security and integrity of the mails, and of all postal property entrusted to them.

271.3 Security Control Officers

271.31 Policy

The installation head or designated manager or supervisor acts as security control officer (SCO) for each facility, including stations and branches. This policy ensures appropriate attention to security issues and facilitates necessary liaison with the Postal Inspection Service.

271.32 Responsibilities

The primary responsibility of the SCO is to ensure the general security of the facility under rules and regulations issued by or concurred in by the chief inspector. This includes the safety of on-duty employees and the security of mail, postal funds, property, and records entrusted to them. The security control officer is also the liaison with the Postal Inspection Service on all security matters and as the individual responsible for implementing security recommendations reported by the Postal Inspection Service.

271.33 Designation

If the security control officer responsibility is delegated by the installation head, the officer must acknowledge, in writing, understanding of the collateral duties of this assignment, as detailed in this chapter. Each Postal Service
district maintains a current list of designated SCOs, their alternates, and phone numbers. Send the appropriate postal inspector in charge a copy of this list. (The inspector in charge also ensures that each SCO has a Postal Inspection Service point of contact and alternate.)

271.34 Duties

271.341 Security Reviews

The SCO or designee conducts annual facility security reviews using the security survey provided by the Postal Inspection Service. Send the completed survey and notes on corrective action taken to the designated Postal Inspection Service liaison. Keep a copy of the survey results at the facility for 2 years.

271.342 Potential Threat or Assault

The SCO must remain sensitive to potential employee threat or assault situations. SCOs should encourage employees to report any situation they feel might lead to physical confrontation or that might affect the safety of the work force. Any employee may make reports to the Postal Inspection Service.

271.343 Safety and Security

The SCO must notify the Postal Inspection Service of any significant situation impacting employee safety or security. Make reports by telephone or in writing, depending on the degree of urgency. A detailed record of all such Postal Inspection Service contacts must be made and kept at the office for 2 years.

271.344 Employee Involvement

The SCO, working with the Postal Inspection Service, ensures that employees are provided appropriate crime prevention and security material and are aware of established security procedures. The need for total employee involvement and participation in the security of their workplace cannot be overemphasized.

271.345 Sensitive Clearance

As necessary, the SCO must do the following regarding sensitive clearances:

a. Ensure that the Postal Inspection Service has granted interim or final sensitive clearance to all employees who require such clearance before allowing them access to the postal areas, documents, or information requiring the clearance.

b. Maintain an accurate, current roster of all employees holding sensitive clearance within their areas of jurisdiction.

c. Obtain from the appropriate personnel office all required forms and data necessary for submission to the Postal Inspection Service when an applicant or transferee is being considered for access to sensitive areas, documents, or information.

d. Ensure that sensitive clearances are updated every 5 years under 272.25.
271.4 **Authorizations**

The Postal Inspection Service evaluates the need for any security-related equipment or personnel. Do not purchase closed circuit television (CCTV) systems, access-control systems, burglar or duress alarms, or fencing without Postal Inspection Service evaluation. The cost of security equipment is a central component of the facility’s construction or renovation budget and becomes part of the building’s assets. The use of on- or off-duty police (or other law enforcement officers) or guard services to provide security at postal facilities requires the consideration of numerous issues. Proposals should be submitted to the Postal Inspection Service with a detailed justification for review and evaluation.

271.5 **Examination and Inspection of Postal Property (Including Lockers)**

All Postal Service-owned or -furnished property under the custody or control of the Postal Service, including that individually assigned to postal personnel, is for official use only. This property and its contents are at all times subject to examination and inspection by duly authorized postal officials in the discharge of their official duties. The chief postal inspector, officers, and heads of installations or their designated representatives are authorized to examine and inspect, as their duties may require, such Postal Service-owned or -furnished property and its contents.

271.6 **Employees**

271.61 **General**

The following responsibilities pertain to the general integrity and security of the mails and the handling of personal mail in the workplace.

*Note:* Refer to 274 for additional mail security requirements.

271.62 **Employee Requests for Mail**

Mail addressed to a postal employee or an employee’s family may not be withdrawn from the mail without approval from a supervisor.

271.63 **Placing Mail on Person or in Personal Receptacles**

Employees must not place mail in their pockets or clothing, in their lockers or desks, or in any other personal receptacles.

271.64 **Employees’ Personal Mail**

271.641 **Guidelines**

Employees must not receive personal mail at their place of employment. Mail that is addressed to an employee at any postal facility’s address is generally considered to be addressed to and intended for the Postal Service, rather than the employee. This mail may be opened by the Postal Service, without the employee’s knowledge or consent, after it is delivered to that facility. Mail that is addressed to an employee at a postal facility’s address and that is
known or appears to be intended for the employee personally may be refused, but must not be opened.

271.642 Exceptions
Exceptions are as follows:

a. Official Postal Service mail or circulars and other mail or circulars that appear to relate to postal employment (such as mail or circulars from the employee unions or from postal uniform vendors) and are intended for individual employees must be delivered without being opened.

b. In the case of an apparent emergency, the Postal Service must accept delivery of personal mail addressed to an employee, and the head of the facility (or designee) must attempt to deliver the mail to the employee.

272 Personnel Security Clearances

272.1 General

272.11 Policy
The Postal Service selects and retains in any capacity only those qualified individuals whose employment is consistent with Postal Service security interests and the national security interests of the United States.

272.12 Responsibility
The chief inspector or designee — referred to here as the personnel security officer — is responsible for the issuance of security clearances. The inspector general is the designee responsible for the issuance of security clearances for all OIG personnel. The inspector general, or designee, is responsible for maintaining an independent program consistent with Postal Service security requirements (272.221 and 272.231), and conducting independent single-scope background investigations. Sensitive clearances for OIG personnel are adjudicated by the inspector general based on information developed during either the initial investigation or an investigation to update a sensitive clearance.

272.13 Scope
Postal Service security interests are activities and matters directly related to the protection of the Postal Service from criminal or other conduct of such a nature as would undermine the safe and efficient movement of the mail or would otherwise undermine Postal Service efficiency or integrity.

272.2 Security Clearances

272.21 Nonsensitive Clearance
Employees requiring nonsensitive clearances are processed under Handbook EL-311, Personnel Operations. On appointment, these employees are the subject of checks conducted by the Postal Inspection Service. These checks are conducted automatically and require no action by the hiring official. Unless disqualifying information is disclosed by the Postal Inspection
Service checks, the individual remains in the position and is cleared for access to such areas, documents, and information as required to accomplish the duties and fulfill the responsibilities of the position.

272.22 **Sensitive Clearance**

Sensitive clearances are considered for Postal Service employees who, by virtue of the duties of their position, have access to sensitive information restricted to the highest levels of the federal government or OIG files, Postal Inspection Service files, national security (classified) information, or sensitive information essential to executive decision making. These employees and executives include:

a. The inspector general, the postmaster general, deputy postmaster general, chief operating officer, the general counsel, the chief inspector, the consumer advocate, the judicial officer, and the vice presidents.

b. Executive secretaries and special assistants to positions listed in 272.22a.

c. The deputy general counsel, chief counsels at Headquarters, and chief field counsels.

d. Any employee required to have knowledge of and access to information or material classified TOP SECRET under Executive Order 12958, Classified National Security Information, dated April 20, 1995, and successive orders.

e. Any employee assigned duties requiring knowledge of the mission of or access to the Federal Emergency Management Agency's (FEMA) Mt. Weather Emergency Assistance Center (MWEAC) or to FEMA emergency preparedness communications equipment or operational documents.

f. All employees of the Office of Inspector General.

g. All employees of the Postal Inspection Service.

h. All Information Systems Service Center (ISSC) managers, ISSC systems security officers, and ISSC security control officers.

i. Finance manager, investment specialists, cash management specialists, financing specialists, and treasury services specialists.

j. District Information Systems manager.

k. EDP Systems Operations supervisor.

l. EDP system coordinator and Information Systems coordinator.

m. Security Control Officers at major plants, offices, and facilities identified by the Postal Inspection Service.

n. Any other employee who is able, by virtue of the duties of a position, to bring about a material adverse effect on the Postal Service or the national security. (The fact that duties may include access to sensitive information does not in and of itself require an individual to have a sensitive clearance.)
272.221 **National Security Positions**

These positions are those concerned with protection of the nation from foreign aggression or espionage, including development of defense plans or policies, intelligence or counterintelligence activities, and related activities concerned with preservation of the military strength of the United States. When a position requires use of, or access to, classified information, national security considerations are ordinarily present. Candidates applying for national security positions must complete Standard Form 86, *Questionnaire for National Security Positions* (revised September 1995).

272.222 **Public Trust Positions**

Public trust positions require the completion of SF 85-P, *Questionnaire for Public Trust Positions* (revised September 1995). These positions are those whose incumbents:

a. May affect the integrity, efficiency, and effectiveness of assigned government activities by their action or inaction. The potential for adverse effect includes action or effectiveness of government, whether or not actual damage occurs.

b. May fulfill certain government activities that by their nature can be adversely affected by the action or inaction of most employees associated with the activity in any responsible capacity. Such activities include law enforcement, public safety and health, collection of revenue, and regulation of business, industry, or finance.

c. Have the authority to commit government funds through grants, loans, loan guarantees, or contracts.

d. Are responsible for managing programs or operations that require a high degree of public trust because of their ability to affect the accomplishment of the activity’s mission to a significant degree. Included in this category are positions responsible for managing a significant portion of a program, such as a geographic district or area.

272.223 **Determining Need for Sensitive Clearance**

When a question is raised about the need for the incumbent of a new position or a position for which the scope of duties has changed to have sensitive clearance, the appropriate security control officer prepares Form 2015 as soon as possible. The SCO sends this form in duplicate to the chief inspector. The form is usually returned to the security control officer within 10 working days.

272.224 **Initiating Sensitive Clearance**

The SCO, through liaison with the appropriate personnel office, initiates clearance processing of an employee or applicant and provides the following documents:


b. Standard Form 87, *Fingerprint Chart*.


d. Notice 70, *U.S. Postal Service Privacy Act Notice*. 
272.225 **Career Postal Service Employees Changing to Sensitive Position**

SCOs submit Standard Form 85-P or Standard Form 86 and Form 2013, *Sensitive Security Clearance Processing Request*, for career Postal Service employees changing to a sensitive position.

272.226 **Processing**

The SCO instructs the employee or applicant to return the completed form in a sealed envelope. Form 2013 is completed by the officer and attached to the outside of the envelope. The officer then forwards the sealed envelope, with Form 2013, to the Postal Inspection Service for investigation at least 10 days before the appointment is planned.

272.227 **Granting Sensitive Clearance**

On completion of a favorable full-field investigation, the chief inspector or designee issues the final sensitive clearance by endorsing and returning the original Form 2013 to the requesting SCO. Concurrently, a copy of Form 2013 is endorsed and returned to the appropriate personnel office for inclusion in the subject’s official personnel folder. Final personnel processing for appointment or assignment of the subject to the position may then be initiated.

272.23 **Denial or Revocation**

272.231 **Criteria**

A sensitive clearance may be denied or revoked by the chief inspector based on information developed during either the initial investigation or an investigation to update a sensitive clearance. The denial or revocation is based on appraisal of circumstances surrounding serious incidents involving the employee or applicant related to the following:

a. Intentional falsification, deception, or fraud in connection with application or examination for appointment or in connection with official inquiry.

b. Refusal to furnish information to the Postal Service requested pursuant to applicable laws, rules, and regulations that would aid in determination of qualification for sensitive clearance.

c. Intentional, unauthorized disclosure or exposure of national security information, documents, or material classified under Executive Order 12065.

d. Any of the other suitability-for-service factors (disqualification reasons) in Handbook EL-311, 313.2.

272.232 **Administrative Procedure to Deny Sensitive Clearance**

When the chief inspector determines that derogatory information developed during an investigation for sensitive clearance falls under the criteria in 272.231 and that the circumstances surrounding the involvement of the subject in the incident do not mitigate the seriousness of the incident, the chief postal inspector sends a memo detailing the disqualifying information to the appropriate operating unit official with a statement that the sensitive clearance is denied.
272.233 Denial Reconsideration
Employees or applicants may request, through the appointing or operating unit official, reconsideration of the denial and present any new information in their own behalf. The chief inspector considers any new evidence presented and advises the appointing or operating unit official of the decision.

272.234 Action of Operating Unit Official
The operating unit official takes the following action:

a. If the chief inspector denies a sensitive clearance to an employee, the responsible official takes steps to do one of the following:
   (1) Remove the employee from the Postal Service under the currently applicable regulations of the Postal Service, Office of Personnel Management, or collective bargaining agreement, as appropriate.
   (2) Reassign the employee to duties that do not require sensitive clearance.
   (3) Refer the case to the postmaster general for a final determination. Provide a copy of the referral to the chief inspector.

b. If the individual is to be retained in the Postal Service, the operating unit official furnishes the chief inspector a written statement of the reasons for retention, with copy to the records officer.

272.24 Interim Sensitive Clearances

272.241 Applicants in Private Industry
When there is a priority need to make a hiring commitment to an individual who requires a sensitive clearance but is not currently employed by any agency or department of the U.S. Government, a request for an interim sensitive clearance may be made. The request is made by checking the appropriate block on Form 2013 and is accompanied by a memorandum signed by the operating unit head. The memorandum must contain full justification for the request and, along with the Form 2013, be accompanied by all completed forms listed in 272.224. All forms must be submitted at least 10 working days before the expected appointment date. If approved, the signed and dated Form 2013 is returned to the appropriate security control officer within 10 working days with the Interim Sensitive Clearance Granted block checked. This endorsement allows the individual to start work. After granting the interim sensitive clearance, the remainder of the investigation is continued without further action required from the security control officer. The final sensitive clearance is granted on favorable completion of the investigation.

272.242 Federal Government Employees
An interim sensitive clearance is normally granted within 10 working days after request and receipt of all forms listed in 272.224 to allow hiring of an individual currently employed by any agency or department of the federal government whether or not the individual holds any security clearance with that agency or department. This also applies to individuals in the Postal Service not holding sensitive clearance but being considered for assignment to duties requiring the clearance. The remainder of the investigation is...
continued without further action required on the part of the security control officer.

272.243 Expedited Procedures
To hasten security processing and allow appointment of an individual to a position requiring sensitive clearance, expedited procedures have been established to complete the following critical portions of the background investigation. The following constitute expedited security processing:

a. Investigative History File (IHF) and National Crime Information Center (NCIC) checks.
b. Review of employment record and reason for leaving last position.
c. Police and credit checks in all cities of residence during the previous 5 years.

272.244 Final Clearance
A final sensitive clearance is granted on favorable completion of the investigation.

272.25 Updating Sensitive Clearances
Five years after the granting of a sensitive clearance, and at least once during each succeeding 5 years, or at the chief inspector’s direction, each individual holding a sensitive clearance must complete Form 2066, Updated Personnel Security Questionnaire, and Form 2181, Authorization and Release. The Postal Inspection Service notifies the appropriate SCO when the updated clearances are due. The SCO makes sure that the employee completes the forms and that the forms are promptly returned to the Postal Inspection Service. On favorable completion of appropriate checks, a copy of Form 2066 is endorsed and returned to the SCO. A copy is also placed in the individual's official personnel folder. The Postal Inspection Service update includes the following:

a. Review of official personnel folder.
b. NCIC (wants and warrants).
c. Criminal history inquiry (cities of residence during past 5 years).
d. Credit check.
e. IHF check.

272.26 Exceptions
When the postmaster general determines that an exception to the foregoing regulations promotes the efficiency of the Postal Service or serves the best interests of the national security of the United States, the postmaster general may grant such an exception.

272.3 Clearances for Individuals Under Service Contracts
272.31 General
272.311 Who Must Have Clearances
Individuals who provide contract services to the Postal Service, including contractors, contractors’ employees, subcontractors, and subcontractors’
employees at any tier, who have access to occupied postal facilities and/or to postal information and resources, including postal computer systems must obtain clearance from the Postal Service, as provided in 272, before being provided that access.

**272.312 Exceptions**

This section does not apply to contractors providing services (including repairs and alterations) under local buying authority or to individuals providing mail transportation services under contract. (See MI PO-530-91-8, Screening Mailhandling Contract Employees, for screening procedures for mail transportation contracts.) For contractors providing services under local buying authority, the postal manager must take reasonable security precautions before allowing these individuals to enter a postal facility, such as examining their past job performances, local criminal histories, and knowledge of their respective companies. To the extent possible, these individuals should have access to facilities only when postal employees occupy the facility.

**272.313 Temporary Services Companies**

Temporary service company contractors (e.g., Manpower, Kelly) are intended to provide short-term support services (e.g., custodial, secretarial, and administrative services). When emergent support services are required, the contractor must provide certification to the contracting officer, COR, or a designee, that the contractor’s employee has met the basic security clearance requirements. If the contractor’s employee requires a higher-level security clearance, the contractor’s employee may work for 2 weeks under the basic clearance, pending approval of the higher clearance.

**272.32 Requirements**

**272.321 Levels of Clearance**

As outlined below, four levels of clearance — basic, nonsensitive, sensitive, and interim sensitive — are available:

a. Basic clearance — Clearance required for individuals who have access to postal facilities, but who do not require a higher level of clearance as provided herein.

   **Exception:** Individuals whose access would otherwise require a basic clearance do not require it if they need to have access for less than 2 weeks. Clearance is required if access is extended beyond 2 weeks.

b. Nonsensitive clearance — Clearance required for individuals who have access to postal information, that if compromised, would have limited impact on the mission of the Postal Service, or who have restricted access to postal computer systems, such as for word processing or data entry.

c. Sensitive clearance — Clearance required for individuals who have access to sensitive information that, if compromised, would cause significant financial loss, inconvenience, or delay in the performance of the mission of the Postal Service, or who have physical access to restricted areas in postal facilities such as computer rooms and tape libraries, or who have access to computer systems such as on-site or
remote terminals for systems development or accessing sensitive systems or data.

**Exception:** Individuals whose access would otherwise require a sensitive clearance require only a nonsensitive clearance if they are assigned to a contract for 60 days or less.

d. Interim sensitive clearance — Preliminary clearance granted for individuals for whom there is a priority need to begin work before the completion of a sensitive clearance.

### 272.322 Citizenship

Individuals requiring a nonsensitive clearance, sensitive clearance, or interim sensitive clearance must be United States citizens, except that permanent resident aliens and other citizens of foreign countries may provide services with the prior approval of the Postal Career Executive Service (PCES) manager for whom the services are required.

### 272.33 Responsibilities

#### 272.331 Contracting Officer, Requiring Activities, and Contracting Officer’s Representative

The organizations requiring contract support and the contracting officer review the scope of work to determine whether the nature of the work requires contracted individuals to have a clearance pursuant to these procedures. If so, a provision referencing these requirements and procedures is included in the solicitation documents. At the time of contract award, the contracting officer, the contracting officer’s representative (COR), or a designee provides the contractor with the required clearance forms and receives the forms upon completion.

a. **Basic clearance** — The contracting officer, the COR, or a designee may allow individuals needed immediately by postal management to have limited access to the postal facility for up to 2 weeks, under the supervision of a postal employee, pending the receipt of the completed certifications for the basic clearance. Upon receipt, the contracting officer, the COR, or a designee reviews them for completeness and adequacy. If the information provided is satisfactory, the contracting officer, the COR, or a designee authorizes the issuance of an identification badge (Form 5140, *Non-Postal Service Contractor Employee*) to the contract employee.

b. **Nonsensitive, sensitive, and interim sensitive clearances** — Upon receipt of the completed forms for the nonsensitive, sensitive, and interim sensitive clearances, the contracting officer, the COR, or a designee reviews them for completeness and adequacy and forwards them to:

SECURITY CLEARANCES
US POSTAL INSPECTION SERVICE
225 N HUMPHRIES BLVD
4TH FLOOR SOUTH
MEMPHIS TN 38161-0008
Individuals requiring a nonsensitive clearance, sensitive clearance, or interim sensitive clearance may begin work when they receive notification that the security clearance has been granted. The contracting officer, the COR, or a designee authorizes the issuance of an identification badge (Form 5140) to the contract employee.

272.332 Postal Inspection Service
The Postal Inspection Service Operations Support Group (ISOSG) performs the following record checks before granting clearances. The ISOSG notifies the contracting officer, the COR, or a designee by memorandum when an individual has been granted or denied a security clearance. When contractor access to a computer is involved, the computer system security officer is also notified.

a. Before granting a nonsensitive, sensitive, or interim clearance, the ISOSG searches the Postal Inspection Service’s data bases.

b. Before granting a nonsensitive, sensitive, or interim clearance, the ISOSG searches the National Crime Information Center (NCIC) Wants and Warrants.

c. Before granting a sensitive clearance, the ISOSG requests a National Agency Check (NAC) from the Office of Personnel Management (OPM) that includes the following:

(1) *Security/Suitability Investigation Index (SII)* — Index of background investigations, those that are completed by OPM and those conducted by other federal investigative agencies. OPM file retention is 15 years, or 25 years for an investigation that contains actionable information.

(2) *FBI Identification Division* — Fingerprint index of arrest records and name file.

(3) *Defense Clearance and Investigation Index (DCII)* — Index of investigations conducted on Department of Defense civilian and military personnel.

272.34 Documentation
272.341 General
If an individual has a current security clearance from another federal agency, the contractor should provide documentation from that federal agency describing the clearance granted, the date it was granted, and the name and telephone number of an agency contact person.

272.342 Basic Clearance
Contractors employing individuals who require a basic clearance must provide the documentation (see 272.341) to the contracting officer, COR, or a designee, before individuals are authorized to enter a postal facility in connection with contract performance. The contractor must also maintain supporting documentation for drug screening tests and criminal history.
272.343 Audits and Investigations

inquiries subject to review by the Postal Service. Contractors must provide certification that each individual:

a. Has passed a screening test for cocaine, marijuana, amphetamine/methamphetamine, opiates, and phencyclidine (PCP), which the Substance Abuse and Mental Health Services Administration (SAMHSA) has identified as the five most abused substances. The screening test must be performed by a SAMHSA-approved, certified laboratory and must meet the cut-off levels established by SAMHSA. The certification must include the name of the employee, the name of the institution that performed the test, the name of the agency that certified the laboratory, the date of the test (within 90 days of the submission of the results), and the negative results of the test.

b. Is not on parole, probation, or under suspended sentence for commission of a felony.

c. Has not been convicted of a criminal violation during the past 5 years for offenses that involved dishonesty, moral turpitude, financial gain, or assault.

d. Has not engaged in the illegal use, possession, sale, or transfer of narcotics or other illicit drugs during the past 5 years.

e. Does not have pending serious criminal charges such as murder, rape, robbery, burglary, physical assaults, sale and distribution of drugs, or weapons violations. If criminal charges are pending, the basic clearance is not to be authorized until the charges have been resolved.

272.343 Nonsensitive Clearance

Contractors employing individuals who require a nonsensitive clearance must provide to the contracting officer, the COR, or a designee the following documentation for each individual before these individuals are authorized to enter a postal facility in connection with contract performance:

a. Form 2181-C, Authorization and Release — Background Investigations (USPS Contractors and Employees of Contractors).

b. Form 1357, Request for Computer Access (if access to postal computer systems is required).

c. Results from a criminal history inquiry through local agencies (in this preferred order — state, county, city), where the individual has resided and has been employed during the past 5 years.

d. Results of a credit bureau inquiry to identify any derogatory financial information concerning the individual.

e. Verification of the individual’s employment history for the past 5 years, including a list of reasons for termination or resignation from prior employers.

f. Verification of the individual’s United States citizenship through review of a birth certificate or naturalization document.

g. Certification that the individual has passed a drug screening test pursuant to procedures for a basic clearance.

h. Form 2025, Contract Personnel Questionnaire.
272.344 **Sensitive Clearance**

Contractors employing individuals who require a sensitive clearance must provide documentation to the contracting officer, the COR, or a designee for each individual before that individual is authorized to enter a postal facility in connection with contract performance.

*Exception:* The initial submission of information required for individuals who had been previously granted a sensitive clearance and who have had a break in service of 6 months or less is to be handled on a case-by-case basis. The complete screening process is required for an individual that has had a break in service of 6 months or more. The documents needed are:

- Items 272.343a through 272.343g listed above for the nonsensitive clearance.
- Form 2013, *Sensitive Security Clearance Processing Request.*
- SF 85-P, *Questionnaire for Public Trust Position.*
- FD 258, *Fingerprint Chart — Applicant* (two copies). The fingerprint cards must be signed and dated by someone with experience taking fingerprints.

272.345 **Interim Sensitive Clearance**

When individuals are to begin work under an interim sensitive clearance, contractors must initially provide the contracting officer, the COR, or a designee with items 272.343c through 272.343g required pursuant to procedures for the nonsensitive clearance (discussed in 272.343) for each individual before authorization can be granted to enter a postal facility in connection with contract performance.

272.35 **Grounds for Denial or Revocation**

A sensitive, nonsensitive, or interim clearance can be denied or revoked based on the information developed during either the initial investigation or an investigation to update a clearance. The denial or revocation can be based on an appraisal of circumstances surrounding serious incidents involving the individual, regardless of the time frame, related to the following:

- Refusal to furnish information requested pursuant to applicable laws, rules, and regulations that would aid in the determination of qualifications for a security clearance.
- Intentional, unauthorized disclosure or exposure of national security information, documents, or material classified under Executive Order 12065.
- Dismissal from prior employment for cause.
- Prior criminal conduct that could undermine the efficiency of the Postal Service or the safety of postal employees.
- Intentional false statements, deception, or fraud in an application for clearance or in a submission of information furnished incidental to a contract with the Postal Service.
- Habitual use of intoxicating beverages to excess.
- Use of narcotics or dangerous drugs.
h. Reasonable doubt as to the loyalty to the government of the United States.

i. Conviction for theft, embezzlement, or crimes of violence, including assault with a deadly weapon.

j. Any other circumstance that makes the individual unfit to do business with the Postal Service.

272.36 Reconsideration of Denial
An individual employed by a contractor, through the contractor, may request that the denial of a request for a clearance be reconsidered, and may present new information on his or her behalf. The chief inspector considers any new evidence presented and advises the contracting officer of the decision. The contractor’s remedies for the failure of the Postal Inspection Service to grant a requested clearance, either initially or following reconsideration, are to be provided in the contract.

272.4 Hiring and Accession Requirements
272.41 Employees Requiring Sensitive Clearance
Individuals who are required to have a sensitive clearance may not enter on duty nor assume duties requiring sensitive clearance until they have been granted either interim or final sensitive clearance by the chief inspector or designee.

272.42 Mail Transportation Contractors
Contractors and their employees engaged in the transport of mail matter or who are allowed access to postal operational areas are not allowed such access unless the proper identification badge is displayed (Form 5139, Nonpostal Service Temporary Employee, or Form 5140, Nonpostal Service Contractor Employee).

273 Facility Security
273.1 Protection and Access
273.11 Requirement
273.111 Responsibilities
Responsibilities are as follows:

a. The Postal Inspection Service establishes the criteria for security of on-duty employees and the security of mail, postal funds, property, and records entrusted to them.

b. The installation head is responsible for implementing recommendations and requesting funds for security equipment and building modifications, and maintaining and upgrading, as necessary, all security and criminal investigative equipment.
273.112 **Facility Planning Concept**

To ensure that the Postal Inspection Service has an opportunity to address the specific security requirements for every Postal Service-owned or -leased facility, advise the inspector in charge in writing on implementation of a facility planning concept. Coordination with the Postal Inspection Service is required throughout the planning, design, and construction phases of every facility to ensure that the security requirements are met and that National Fire Protection Association (NFPA) 101 Life Safety Code requirements are not adversely affected.

273.113 **Facility Security Surveys**

The Postal Inspection Service periodically conducts facility security surveys to determine compliance with security requirements. Formal reports with recommendations for necessary security enhancements are submitted to postal management for review and implementation.

273.12 **Workroom Access**

273.121 **Limitations**

Access to all workroom areas is limited to authorized on-duty postal employees and authorized contractors. All other individuals are excluded unless they have legitimate business on the floor and are properly escorted.

273.122 **Door Locks**

Installation heads are required to carefully evaluate the work-flow cycles of their units to determine when the workroom doors can be locked. This is normally at all times except during heavy traffic periods when employees are reporting to or departing from work.

273.123 **Compliance**

The policy governing the locking of doors should be firmly adhered to. Supervision to ensure compliance is necessary to afford maximum protection of postal employees, funds, and property. Emergency egress is to be provided in accordance with the NFPA 101 Life Safety Code.

273.13 **Employee Responsibilities**

273.131 **Unauthorized Individuals**

All employees are charged with the responsibility of preventing unauthorized individuals, including off-duty employees, from entering restricted areas. All individuals on the workroom floor who are not properly identified or escorted should be immediately challenged.

273.132 **Reporting Conditions or Conduct**

To assure postal safety, employees report all unsafe building or working conditions. Employees must also report any disturbances or improper conduct on the part of individuals while on postal premises.

273.133 **Emergency Actions**

In emergencies, employees are to take the following necessary actions:

a. Call for fire or police assistance.

b. Use fire extinguishing equipment.
273.14 Audits and Investigations

c. Assist with the injured.
d. Protect postal assets and mail if there is no risk to employee safety.

273.14 Security Force

The Postal Inspection Service may authorize a security force to provide security at selected postal installations. Where assigned, security force personnel as members of the Postal Inspection Service, are responsible for perimeter and building security. Appropriate liaison between installation heads, postal police officers in charge, and inspectors in charge should be maintained to ensure full coverage of all proper areas of access control and security.

273.15 Police Protection

State and local police agencies are generally willing to assist in protecting postal property. They may inquire about the jurisdictional status of a facility to be sure it allows them access and authority to enforce their laws. Facilities purchased or leased since 1962 are occupied by the Postal Service under proprietary jurisdiction. This term means that state or local police enjoy the same rights there as on any private property, if their activities do not unduly interfere with postal operations. Any police inquiry about status of a facility that came into postal use before 1962 should be forwarded to the inspector in charge.

273.16 Security by Contract

273.161 Policy

The chief inspector or designee, in the capacity of security officer for the Postal Service, is responsible for approving all requests for security contractors.

273.162 Procedures

Procedures vary as follows:

a. Normally, facility managers submit all proposals for the use of security contractors to the local inspector in charge with a detailed justification. The inspector in charge reviews, evaluates, and submits proposals to the chief inspector for consideration. The chief inspector notifies the inspector in charge of the decision. The inspector in charge will notify the facility manager of the decision.

b. In an emergency, facility managers may obtain contract security without prior approval but must notify the local inspector in charge as soon as possible. The inspector in charge must immediately report the emergency hiring of contract security to the chief inspector.

273.163 Union Notification

In accordance with the USPS-FOP Agreement, the national FOP-NLC-USPS No. 2 must be notified within 30 days of the decision to place contract security at any postal facility, unless postal police officers are deployed at that postal facility. If a decision is made to contract security work at a postal facility where postal police officers are deployed, the national FOP-NLC-USPS No. 2 should be notified before the deployment of the contract personnel.
whenever practical. Notice to the national FOP-NLC-USPS No. 2 will be
given at the Headquarters level.

273.17  Closed Circuit Television System Security

273.171  Scope
This section clarifies the use of closed circuit television (CCTV) in
administrative and security applications. It does not affect the manner in
which the Postal Inspection Service or OIG utilizes CCTV equipment for
criminal investigations.

273.172  Policy
The Postal Service uses CCTV systems for the protection of its employees,
mail, and postal assets, and to monitor automated mail flow operations. The
purpose of CCTV systems is to provide visual verification in conjunction with
intrusion detection devices or exit alarms and doors equipped with exit
alarms or access control devices. CCTV systems are to function as
deterrents, and if a crime occurs in the monitored area, to record evidence of
it. The administrative and security uses of CCTV systems are limited to the
following:

a. CCTV systems are installed to view parking lots, building exteriors,
   employee and visitor entrances, other access controlled entrances,
   emergency egress only, post office box areas, public access areas, and
designated high-value locations, such as registry areas.

b. CCTV systems are not installed to view work areas to evaluate the
   performance of employees.

c. CCTV systems do not utilize “dummy” or nonfunctioning CCTV
   cameras.

d. Security in the postal retail store.

273.173  Responsibility
The following units have these responsibilities:

a. Postal Inspection Service — The inspector in charge of the division in
   which the facility is located is responsible for determining the need for,
   quantity, type, and location of CCTV systems and cameras as
   described in this section.

b. Security Control Officer — The security control officer (SCO) is
   responsible for overseeing the procurement, installation, maintenance,
   and repair of CCTV systems, and for maintaining a minimum of the
   most recent 32 days of video recording tapes or disks. The SCO also
   assures that the information from the CCTV camera is monitored
   and/or properly recorded 24 hours a day. At least once a year, one-third
   of the tapes must be replaced.

273.2  Alarms and Sensors
The Postal Inspection Service determines the need for alarm systems.
Alarms and related sensor systems are installed in certain selected postal
facilities to prevent burglary and robbery and/or to assist in the apprehension
of offenders. The inspector in charge gives the facility head detailed
operating instructions for facility alarm systems. These instructions are restricted information and are kept in a secure area. (See Handbook RE-5, *Building and Site Security Requirements*, and Handbook AS-503, *Standard Design Criteria*, for details on design and installation of the systems.) Problems regarding alarm systems should be brought to the attention of the inspector in charge.

273.3 **Security Counter Lines**

Security counter lines are installed in selected facilities for additional protection of employees. Requirements for these bullet resistant screen lines are developed by the Postal Inspection Service. The screen line should provide protection above, below and 10 feet on either side of the counter line. Handbooks AS-503 and RE-5 provide details to design the counter line.

273.4 **Locks, Keys, and Access Control Cards**

273.41 **Responsibility**

Postmasters procure all replacement locks and lock assemblies needed at their facilities, including Postal Inspection Service locks.

273.42 **Postal Inspection Service Locks**

The various locks used only for Postal Inspection Service offices, lookout galleries, and evidence rooms are shown in Exhibit 273.42. These locks are stocked at the Somerville Material Distribution Center. Order Postal Inspection Service locks in accordance with Publication 247, *Supply and Equipment Catalog*.

273.43 **Postal Inspection Service Keys**

273.431 **O Key**

In buildings with lookout galleries, one O key is assigned to the postmaster or other official in charge, who must personally safeguard the key at all times. Only the postmaster or a designated supervisor may admit cleaners or other authorized persons to the galleries, on the first Monday of the month or by obtaining approval in advance from the responsible inspector in charge.

273.432 **J Key**

A special J key, which operates inspectors’ office locks, is provided for other authorized personnel.

273.433 **Ordering Procedures**

Postmasters at facilities having inspectors’ offices and observation galleries must order O keys and special J keys by memo from the inspector in charge. If the order involves replacement of a defective key, return the defective key with the request. Send O and special J keys by registered mail. Report the loss of either of these keys promptly to the inspector in charge.
## Postal Inspection Service Locks

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Federal Spec. Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>912-B</td>
<td>Cylindrical (key-in-knob). Complete kit available in dull stainless steel finish only.</td>
<td>161</td>
<td>In newly constructed buildings, install on corridors opening directly into inspectors’ private offices and on evidence storage room doors. Also use to replace defective cylindrical locks on such doors.</td>
</tr>
<tr>
<td>912-C</td>
<td>Cylindrical (key-in-handle). Complete kit available in dull stainless steel finish only. Operable by special J key used by cleaners. Lever action lock.</td>
<td>161</td>
<td>In newly constructed buildings, install on one door (usually reception office) of inspectors’ office or suite. Also use to replace defective locks of same type on such doors. If inspectors’ private offices are not accessible through interconnecting doors from reception area, install on corridor entrance door of private offices to enable cleaners to enter with special J key.</td>
</tr>
<tr>
<td>912-D</td>
<td>Cylindrical (key-in-knob). Complete kit available in dull stainless steel finish only. Operated by O key assigned to postmaster or other official in charge of building housing a gallery.</td>
<td>161</td>
<td>Use on all interior gallery doors in new buildings and to replace defective 912-A (obsolete) or 912-D locks on such doors.</td>
</tr>
<tr>
<td>0931-AH</td>
<td>Mortise type. Complete kit available in dull stainless steel finish only.</td>
<td>86</td>
<td>In new buildings, use on all exterior doors to inspectors' offices and gallery doors accessible to the general public. Also use to replace defective locks of same type on such doors.</td>
</tr>
<tr>
<td>0931CYL</td>
<td>Rim cylinder keyed for inspector key only.</td>
<td>—</td>
<td>Use with all surface-mounted deadbolt locks.</td>
</tr>
<tr>
<td>091SP</td>
<td>Threaded cylinder only (mortise type). Available only in brass finish.</td>
<td>86</td>
<td>Use as replacement cylinder for defective locks of Series 86 type on lookout gallery doors and inspectors’ private office doors (see also item 912-B).</td>
</tr>
<tr>
<td>0931AO</td>
<td>Threaded cylinder only (mortise type). Available only in brass. Operable by special O key used by cleaners for lookout gallery (LOG).</td>
<td>86</td>
<td>Use as replacement cylinder for defective locks of same type on inspectors’ office doors.</td>
</tr>
</tbody>
</table>
273.434 **Key Log**
All employees needing access to lookout galleries or Postal Inspection Service space must sign for keys in the key log. The log must show requestor names, dates, and key-out and key-in times. Overnight retention of keys is prohibited. Coordinate access for other than scheduled cleaning with the inspector in charge.

273.44 **Postal Service Locks**
273.441 **Exterior**
All exterior doors must be equipped with a deadbolt lock. An American National Standards Institute (ANSI) 156.13 Series F15 or F20 lock is required for employee entrance and single (exterior) doors. The deadbolt feature is operated by key (from the outside) and by turning the lever from inside. When the deadbolt is extended, turning the inside lever retracts both latch bolt and deadbolt simultaneously. On store front doors not designated as egress doors, a keyed both-side hook-type deadbolt is required. (See handbooks AS-503 and RE-5 for further information.)

273.442 **Electronic Strike**
If an ANSI 156.13 F15 lock with a permanent rigid outside knob is installed, an electronic strike may be provided for employee access during the normal business day. The strike may be operated by an interior release button or exterior, electronic cipher keypad. The deadbolt portion of the lock is activated to prevent employee access after hours. Install these locks following standards established by the Occupational Safety and Health Administration (OSHA) 1910.36 and the National Fire Protection Association (NFPA) Life Safety Code (LSC) Section 5-2.1.2.1, 1981 edition. No combination of locking mechanisms may impede the orderly exit of people in the event of an emergency, even in complete darkness.

273.443 **Delayed-Exiting Locks**
Delayed-exiting locks are not an authorized method for securing emergency exit doors. For doors requiring the level of security provided by the delayed-exiting devices, plant managers or their designees should install and subsequently monitor a combination of local and remote annunciators and closed circuit television (CCTV) systems.

273.444 **Access Control System**
For facilities of 20 or more employees a simple, single access control system should be installed. See handbooks AS-503 and RE-5 for details of an access control system design.

273.45 **Postal Service Keys and Access Control Cards**
273.451 **Postal Employees**
Personnel are issued only such keys as their duties require. Entrance lock keys are furnished only to those postal employees who are required to open the office in the morning or close it at night. Management reviews employee key requirements semiannually. They are not on a master key system. Standard locks are not authorized on exterior doors or in high security areas.
273.452 Nonpostal Occupants
Nonpostal occupants may be furnished keys to the entrance doors of their offices when necessary. They may not be furnished keys that allow access to the workroom areas. Other types of building keys may be furnished to nonpostal occupants, providing there is an official need.

273.453 Contractors
Keys may be furnished to highway contractors for exchange of mail in lobbies, vestibules, or lockers of post offices when those offices are not open. These keys must not permit access to workroom areas.

273.46 Key Accountability

273.461 Inventory
Postmasters must keep an accurate inventory (including serial number and brand name of lock, total number of keys available, location of lock by door and/or room number, how and when disposed of) of all building keys and signed receipts for all assigned keys. Signed receipts are obtained using Form 1628, Individual Key Record, when keys are assigned.

273.462 Return of Keys
When an employee’s duties no longer require the use of an assigned key or the employee leaves the service, the key must be returned immediately. The date of return is then entered on Form 1628 as the release of accountability. If keys used to operate exterior doors to the facility are not returned, the locks must be replaced or rekeyed.

273.463 Unassigned Keys
Store all unassigned keys in a secure place accessible only to the postmaster or a designated alternate.

273.464 Key Survey
Conduct a semiannual physical survey of all building keys. Pay particular attention to master keys, exterior entrance keys, and special keys such as those for registry cages, stamped envelope rooms, employee record rooms, etc.

273.47 Reporting Lost or Stolen Keys or Access Control Cards

273.471 Procedures
Immediately report a lost or stolen key or access control card to the inspector in charge. Describe in detail the key or access control card, case, or key chain. If the key is lost to an outside door, immediately exchange the lock cylinder on the entrance door with one from the interior of the building that is not operable by the building master key.

273.472 Postal Inspection Service Keys
Also report lost or stolen regulation lookout gallery O keys, as well as J keys, to the inspector in charge.
273.48 Master Keys

Only postmasters, installation heads, or their designees may carry a master key. At installations having a Postal Service security force, one or more master keys are issued to the ranking postal police supervisor for use by postal police in emergencies. Master keys are issued to maintenance employees only during their tours of duty and may not be carried from the building. No other occupants of the building are issued master keys, and any such keys in the possession of other occupants must be recalled. Master keying is not permitted for locks opening stamped envelope rooms or other locations requiring individual accountability of contents. This applies to exterior doors in retail and delivery facilities.

273.5 Security Containers, Safes, and Vaults

273.51 Security Containers and Safe Equipment

273.511 General

Security containers (Publication 247 items 293 through 299) are furnished to post offices in CAGs A through K and their stations and branches for cash, stamp stock, money orders, food stamps, and other valuable items. Other postal units, including CAG L post offices in quarters furnished by the federal government where the postmaster does not receive an automatic 15 percent of salary for heat, light, and equipment, are furnished surplus fireproof safes or similar appropriate storage equipment consistent with available supplies.

273.512 Description

Requisitioned items 293 through 299 should provide space, if possible, for regular window clerks using standard cash drawers (items 216, 217, 218, or 219), unless cash and stamp drawer cabinets (items 220 or 221) are located in a vault. Otherwise, window clerks should use the cash box (item O911) or be furnished a separate locked compartment in the security container.

273.513 Exception

When the value of office accountability and registered mail regularly exceeds $25,000 and security containers, fireproof safes, or vaults are not provided for overnight storage, contact the inspector in charge.

273.52 Vault Equipment

273.521 Criteria for Use

Using vaults in place of security containers must be considered based on the volume of security storage needed at the facility. Generally, facilities requiring five or more security containers or bulk storage of accountable items require a vault. This does not preclude stamped envelopes and retail products.

273.522 New or Replacement Vault Doors

Vaults built to Postal Service Standard (See Handbook AS-503, Standard Design Criteria) provide better protection than other safekeeping equipment. GSA Class 5 vault doors modified with a Sargent and Greenleaf 8400 series mechanical lock are provided for newly constructed vaults or as replacements for defective or damaged vault doors.
273.523 **Modular Vaults**

Modular vaults meeting Underwriter’s Laboratories (UL) Standard 608 may be substituted for vaults built to other Postal Service standards. Authorized vaults must meet Class M level of security and doors must meet the requirements in section 273.522. Vaults built to Postal Service standards as detailed in Handbook AS-503 provide better protection than other safekeeping equipment.

273.524 **Cash Drawers**

For storing cash drawers in a vault, use items 220 and/or 221 unless space is available in security containers located within the vault.

273.525 **Exception**

For storing cash, postage stamps, money orders, and food coupons in vaults not meeting specifications of 273.522 and 273.523, use security containers, chests, or fireproof safes inside the vault to the extent equipment is available and interior space of vault is sufficient. Items 222 and/or 223 may be used in vaults meeting 273.522 and 273.523.

273.526 **Magnetic Media**

For storing magnetic media such as diskettes, use certified data storage vaults.

273.53 **Requisitions**

273.531 **Procedure**

Requisition all safe, security container, and vault equipment on Form 7381, *Requisition for Supplies, Services, or Equipment*. Justification for equipment must accompany the requisition.

273.532 **Justification**

Include the following in the justification:

a. If standard cash drawers are in use, the number in use and the number that can be stored in existing equipment must be stated.

b. Requisitions for items 220, 221, and/or 223 must show that a Postal Service standard vault is available and that the equipment is to be used in it.

c. In leased or rented quarters or mobile post offices, it must be determined that the floor can support at least 1,300 pounds, and this fact must be stated on Form 7381.

274 **Mail Security**

274.1 **Importance**

The Postal Service must preserve and protect the security of all mail in its custody from unauthorized opening, inspection, or reading of contents or covers; tampering; delay; or other unauthorized acts. Any postal employee committing or allowing any of these unauthorized acts is subject to administrative discipline or criminal prosecution leading to fine, imprisonment, or both. In cases when an employee having a question about proper mail
security procedures cannot consult a supervisor and when the procedures are not clearly and specifically answered by postal regulations or by written direction of the Postal Inspection Service or General Counsel, the employee must resolve the question by protecting the mail in all respects and moving it, or letting it move, without interruption, to its destination.

274.2 Opening, Searching, and Reading Mail Generally Prohibited

274.21 Mail Sealed Against Inspection

No person may open mail sealed against inspection; or search, inspect, read, or disclose information obtained from the mail or its contents; or surrender all or any part of such mail, whether or not such is believed to contain criminal or other nonmailable matter; except to the extent one or more of these actions is permitted because the person is:

a. A postal employee in a mail recovery center acting under the dead mail regulations in \textit{Postal Operations Manual} (POM) 69.

b. A postal employee acting with the consent of the addressee or sender.

c. A person executing a search warrant under 274.6.

d. An authorized U.S. Customs Service or U.S. Department of Agriculture employee acting under 274.91 or 274.92.

e. A postal inspector acting under 274.91d.

f. A postal employee disclosing information under 274.5.

g. An agricultural inspector of a state or territory of the United States, acting under the Terminal Inspection Act (7 U.S.C. 166) and in strict accordance with pertinent procedures in Publication 14, \textit{Restrictions and Prohibitions on Mailing Animals, Plants, and Related Matter}.

h. Acting as otherwise expressly permitted by federal statutes or postal regulations.

274.22 Mail Not Sealed Against Inspection

Mail not sealed against inspection may be opened, and its contents searched, inspected, and read, all or any part of it surrendered, and information obtained from it released, but only to the extent a person is permitted to take one or more of these actions under the following conditions:

a. Under any of the conditions that qualify for an exception under 274.21.

b. By a postal employee, when authorized to make a determination about the mailability of the contents or the applicable postage for unsealed mail.

c. As otherwise expressly permitted by federal statutes or postal regulations.

274.23 Definitions

274.231 Mail Sealed Against Inspection

The following terms and definitions apply:

a. For purposes of this part, the terms “mail sealed against inspection” and “sealed mail” mean mail on which appropriate postage is paid, and
which, under postal laws and regulations, is included within a class of mail maintained by the Postal Service for the transmission of letters sealed against inspection.

b. The terms include First-Class Mail, Priority Mail, Express Mail (domestic and international), Mailgram messages, and the international letter mail forming part of the LC class of Postal Union mail. See the definition of Postal Union mail in the *International Mail Manual*.

c. The terms exclude incidental First-Class matter permitted to be enclosed in or attached to certain Periodicals, Standard (A) and Standard (B) mailings (see DMM E070) and international transit mail (see 274.8).

d. When sealed mail is part of a mixed class mailing (see DMM E070), the sealed mail component of the combination item is treated as sealed mail only if it is contained in its own envelope or other form of sealed container.

274.232 **Mail Not Sealed Against Inspection**

The following terms and definitions apply:

a. For purposes of this part, the terms “mail not sealed against inspection” and “unsealed mail” mean mail on which appropriate postage for sealed mail is not paid, and which under postal laws or regulations is not included within a class of mail maintained by the Postal Service for the transmission of letters sealed against inspection.

b. The terms include Periodicals, Standard Mail, incidental First-Class attachments or enclosures mailed under DMM E070, and (as defined in the *International Mail Manual*) international parcel post mail, the AO class of Postal Union mail, and the international post cards and postal cards forming part of the LC class of Postal Union mail.

c. The terms do not include international transit mail (see 274.8).

274.24 **Correspondence in Unsealed Mail**

The contents of correspondence permitted to be sent by the blind in special or raised characters, or in the form of sound recordings, and by schoolchildren at the international printed matter rate, must not be divulged except to a postal employee acting with the consent of the addressee or sender, or to a person executing a search warrant under 274.6.

274.3 **Permissible Detention of Mail**

274.31 **Sealed Mail Generally Not Detained**

No one may detain mail sealed against inspection (other than a postal employee detaining dead mail), except under the following conditions:

a. A postal inspector acting diligently and without avoidable delay, upon reasonable suspicion, for a brief period of time, to assemble evidence sufficient to satisfy the probable-cause requirement for a search warrant under 274.6.

b. A postal inspector acting under 39 U.S.C. 3003 who causes to be withheld from delivery mail that he or she believes is involved in a
scheme described in that statute if prompt written notice is given to the addressee advising the addressee of such action, the reasons for the action, and the addressee’s right to have such action reviewed under 39 CFR 964.

c. A postal inspector acting under 39 U.S.C. 3004 who causes to be withheld from delivery letters or parcels sent in the mail to places not the residence or regular business address of the person to whom they are intended to enable the person to escape identification, if prompt written notice is given to the addressee advising the addressee of such action, the reasons for such actions, and the addressee’s right to have such action reviewed under 39 CFR 964.

d. A postal inspector, OIG personnel, or postal employee upon reasonable suspicion and in strict compliance with postal regulations to determine the mailability of injurious articles and substances proscribed by DMM C021, or the proper payment of postage.

e. A postal employee acting under postal regulations with the addressee’s or sender’s express consent (for example, DMM D030).

f. A postal employee acting under an order issued under 39 U.S.C. 3005, relating to false representations, lotteries, and unlawful matter.

g. A postal employee acting under 274.62.

h. A postal employee conducting a mail count by direction of a postmaster or a postal inspector.

i. A postal employee acting under a federal court order.

j. A postal employee, during the period required to seek and obtain instructions under DMM D042.6.0 concerning mail whose delivery is in dispute, or under 424.1 of the Postal Operations Manual (POM) concerning legal process, other than a search warrant duly issued under Rule 41 of the Federal Rules of Criminal Procedure, purporting to require the surrender of mail matter.

k. A postal employee or an agricultural inspector of a state or territory of the United States, acting under the Terminal Inspection Act (7 U.S.C. 166) and in strict accordance with pertinent procedures in Publication 14, Restrictions and Prohibitions on Mailing Animals, Plants, and Related Matter.

274.32 **Unsealed Mail**

Mail not sealed against inspection may be delayed or detained for the reasons in 274.31, and as otherwise expressly permitted by postal regulations.

274.4 **Mail Reasonably Suspected of Being Dangerous to Persons or Property**

274.41 **Screening of Mail**

When the chief postal inspector determines that there is a credible threat that certain mail may contain a bomb, explosives, or other material that would endanger life or property, the chief postal inspector may, without a search...
warrant or sender’s or addressee’s consent, authorize the screening of such mail by any means capable of identifying explosives, or other dangerous contents in the mails. The screening must be within the limits of this subsection and without opening mail that is sealed against inspection or revealing the contents of correspondence within mail that is sealed against inspection. The screening is conducted according to these requirements:

a. Screening of mail authorized by this subsection must be limited to the least quantity of mail necessary to respond to the threat.

b. Such screening must be done in a manner that does not avoidably delay the screened mail.

c. The chief postal inspector may authorize screening of mail by postal employees and by persons not employed by the Postal Service under such instructions that require compliance with this part and protect the security of the mail. No information obtained from such screening may be disclosed unless authorized by this part.

d. Mail of insufficient weight to pose a hazard to air or surface transportation and international transit mail must be excluded from such screening.

e. After screening conducted under this subsection, mail that is reasonably suspected of posing an immediate and substantial danger to life or limb, or an immediate and substantial danger to property, may be treated by postal employees as provided in 274.42.

f. After screening, mail sealed against inspection that presents doubts about whether its contents are hazardous, that cannot be resolved without opening, must be reported to the Postal Inspection Service. Such mail must be disposed of under instructions promptly furnished by the Postal Inspection Service.

274.42 **Threatening Pieces of Mail**

Mail, sealed or unsealed, reasonably suspected of posing an immediate danger to life or limb or an immediate and substantial danger to property may, without a search warrant, be detained, opened, removed from postal custody, and processed or treated, but only to the extent necessary to determine and eliminate the danger and only if a complete written and sworn statement of the detention, opening, removal, or treatment, and the circumstances that prompted it, signed by the person purporting to act under this subsection, is promptly forwarded to the chief postal inspector.

274.43 **Reports**

Any person purporting to act under this subsection who does not report his or her action to the chief postal inspector under the requirements of this subsection, or whose action is determined after investigation not to have been authorized, is subject to disciplinary action or criminal prosecution, or both.
274.5 Disclosure of Information Collected From Mail Sent or Received by Customers

Except under 274.5a through 274.5g, no employee may, in the performance of official duties, disclose information on the cover of a piece of mail; information from the contents of a piece of mail inspected as authorized; or other information about a piece of mail sent or received by any sender, addressee, or group of senders or addressees. An employee may disclose such information:

a. To the Postal Inspection Service or OIG for its official use, including appropriate reference to law enforcement authorities, when there is a reasonable basis to suspect that such information is evidence of the commission of a crime. This exception does not apply to information obtained by opening sealed mail in a mail recovery center, as that information may be used only in seeking to identify an address at which the mail can be delivered.

b. Under 213 regarding mail covers.

c. Under a search warrant in accordance with 274.6.

d. Under a federal court order.

e. At the request of the sender or addressee, or the authorized agent of either.

f. From the covers of mail by films or photocopies of the covers only for the following postal operations:

   (1) Resolving or recording a service complaint when the complaining customer presents the cover as evidence.

   (2) Serving in place of Form 3546 if the film or copy shows nothing but the addressee's prior and current addresses, and does not reveal the sender's name and address, the postmark, or any other information.

   (3) Serving in place of Form 3547 by showing the cover with an address-correction label affixed in reply to a mailer's request for address correction on First-Class Mail and Standard Mail (A) or (B).

   (4) Notifying a mailer of addressing inaccuracies affecting optical character reader (OCR) readability if the film or copy is secured in a locked cabinet, then destroyed as soon as the mailer resolves the inaccuracies.

   (5) Facilitating internal postal operations under specific authorization from the chief postal inspector and written instructions from the records officer not to disclose the information outside the Postal Service, and to destroy the film or copy after a given retention period.

   (6) Resolving a problem of machine missorting or of miscoded or unreadable OCR mail if the information is disclosed only to the postal employees resolving the problem and that the copy is destroyed immediately after resolution of the problem.
(7) Resolving a problem that involves Express Mail and is based on a complaint from the sender or addressee, a refund request from the sender, or an internal service report if the information is disclosed only to the postal employees resolving the problem and that the film or copy is destroyed immediately after resolution of the problem.

(8) Providing information to a Postal Service contractor in the performance of a contract with the Postal Service, but only if disclosure is authorized by the chief postal inspector and use of the information is in strict compliance with contract clause 1-7, Non-Disclosure of Address Information (Appendix B of the Purchasing Manual).

g. From the covers of mail to document the mailing of an item that has, or is reasonably suspected of having, improper postage of any kind. This subsection may be used only by OIG personnel, a postal inspector, or by a postal employee acting at the direction of OIG personnel or a postal inspector. Any documentation must be destroyed when it is no longer needed for official use.

h. To Customs or Agriculture agencies under §274.9.

i. If otherwise permitted by postal regulations.

274.6 Execution of Search Warrants

274.61 Warrant Issued by Federal Court or Served by Federal Officer

a. A search warrant duly issued under Rule 41 of the Federal Rules of Criminal Procedure must be executed as provided in 274.62. Usually, a warrant issued by a federal court or served by a federal officer is issued under Rule 41, and is duly issued if signed and dated within the past 10 days.

b. No employee may permit the execution of a search warrant issued by a state court and served by a state officer. If in doubt, an employee should temporarily detain the mail in question and promptly call a postal inspector for guidance.

274.62 Search Warrant Execution Procedures

Procedures for executing a search warrant follow:

a. A postal inspector may execute a search warrant.

b. An OIG special agent may execute a search warrant.

c. A person other than a postal inspector or OIG special agent executing a search warrant must be accompanied by a postal employee authorized by the head of the postal installation at which the warrant is to be executed.

d. Mail may be taken from postal custody under the authority of a search warrant only if the person executing the warrant leaves a copy of the warrant and a receipt or inventory, made out in the presence of the postal employee accompanying that person, which particularly describes each piece of mail taken, including all service endorsements.
on the cover (such as “Return Receipt Requested”) and any official postal identity numbers (such as registry, insurance, or certified mail numbers). The receipt or inventory may be attached to the copy of the warrant or written on the reverse side of the copy of the warrant.

e. The installation head or designee must do the following:

   (1) Make a copy of the receipt or inventory, and of the copy of the warrant, and send them to the inspector in charge of the division in which the installation is located.

   (2) Send a report of the seizure of any domestic mail to the addressee’s post office and of any seized international mail to the appropriate international claims office.

274.63 Notice to Sender or Addressee

If the cover of domestic mail has been endorsed and stamped to show that the sender has requested and paid for a return receipt, the sender must be notified of the seizure of the mail under the warrant by an endorsement to that effect on the return receipt or on a duplicate, if the original receipt is taken. The receipt must be dispatched as soon as possible, unless the officer executing the warrant presents a federal court order to delay the dispatch. In that event, the dispatch must be delayed in accordance with the order.

274.7 Cooperation With Federal, State, and Local Agencies

A postal employee receiving a request from a federal, state, or local law enforcement, intelligence, or other government agency, for access to, or information about, particular mail matter of any class in the custody of the Postal Service must refer the request to the Postal Inspection Service. The employee must include an explanation that the Postal Inspection Service is responsible for liaison with all government agencies with respect to a request of this kind. No employee of the Postal Inspection Service may comply with such a request, unless authorized by postal regulations.

274.8 International Transit Mail

274.81 Definitions

274.811 International Transit Mail

As used in this part, the term “international transit mail” refers to mail of foreign origin that is passed by a foreign postal administration to the Postal Service for forwarding to a foreign postal administration under a postal treaty or convention. It includes closed mail and à découvert letter post items (see 274.813).

274.812 Closed Mail

The term “closed mail” refers to any bag, container, or mail passed to the Postal Service by a foreign postal administration, the entire contents of which are required, by applicable postal treaties or conventions, to be passed to a foreign postal administration.
274.813 À Découvert Letter Post Item
The term “à découvert letter post item” refers to any international letter post item (Postal Union mail, as defined in the *International Mail Manual*) that is addressed for delivery by a foreign postal administration and is passed to the Postal Service by a foreign postal administration in a bag, container, or mail that must be opened by the Postal Service under applicable postal treaties or conventions because it also contains items addressed for delivery by the Postal Service.

274.82 Special Security Rules
International transit mail is entitled to freedom of transit. It must not be opened, seized, or searched. It is not subject to Customs or Agriculture inspection under 274.91 or 274.92. In accordance with the Universal Postal Convention, any international transit mail consisting of closed mail, à découvert letter post items, and airmail correspondence must not be detained, but must instead be forwarded to the next foreign postal administration by the quickest routes that the Postal Service uses for mail sealed against inspection.

274.9 Mail Security, Law Enforcement, and Other Government Agencies

274.91 Customs Service
Without a search warrant, but upon reasonable cause to suspect that the mail contains dutiable or prohibited items, designated personnel of the U.S. Customs Service may open or inspect the contents of mail in the customs inspection of mail (including APO and FPO mail) that originated outside the Customs Territory of the United States (CTUS) and is addressed for delivery either inside the CTUS or inside the customs district of the Virgin Islands, on the following terms and conditions:

a. *Other Regulations* — Such inspections may be conducted only under the *International Mail Manual* (IMM) relating to cooperation with the U.S. Customs Service on inspection of imports.

b. *Privacy of Correspondence* — No Customs personnel may read, allow any other person to read, divulge, or transfer to any other person any correspondence contained in sealed mail; nor may Customs personnel divulge, allow any other person to read or listen to, transfer to any other person, or knowingly listen to any paper or recording that is correspondence for the blind contained in unsealed mail; nor may Customs personnel divulge, allow any other person to read, or transfer to any person correspondence of school children permitted transmission in unsealed mail, unless such action is authorized by a search warrant issued under Rule 41 of the Federal Rules of Criminal Procedure.

c. *Search Warrant Required for Domestic and Certain International Mail* — No Customs personnel may, without a search warrant, open, inspect, read, or seize any mail in postal custody (including APO and FPO mail) that has not originated outside the CTUS, or that has
Audits and Investigations

diplomatic or consular immunity from Customs inspection (see IMM 711).

d. **Controlled Delivery of Drugs in Sealed Mail** — When a postal inspector decides, at the request of a federal, military, state, or local narcotics agent, to make a controlled postal delivery of a sealed mail article that the Customs Service has opened under 274.91, and that the Customs Service has determined through a reliable field test or reliable laboratory examination to contain illegal narcotics or dangerous drugs, the postal inspector may reopen the article without a search warrant. The inspector may reopen the article without a warrant only to prepare the article for such a controlled delivery in such way or ways as lawfully and reasonably aid in the investigation of the crime of importing such substances through the mail. No correspondence inside such an article may be read or divulged without a search warrant as described in 274.6.

274.92 **U.S. Department of Agriculture**

274.921 **Foreign Origin Mail**

Without a search warrant, but with the written consent of the sender, designated personnel of the U.S. Department of Agriculture (USDA) may open and inspect (but not read) the contents of mail (including APO and FPO mail) that has originated outside the Customs Territory of the United States (CTUS) and is addressed for delivery inside the CTUS. Such inspection may be conducted only under IMM 720 relating to cooperation with the USDA on plant quarantine inspections of imports.

274.922 **Domestic Mail From Hawaii or Puerto Rico**

Without a search warrant, designated USDA personnel may open and inspect (but not read) the contents of mail reasonably suspected of containing plant matter or plant pests mailed in Hawaii or Puerto Rico and addressed to the United States mainland, either with the consent of the sender or if the mail is unsealed. Such inspections may take place only in designated areas of the Hawaii or Puerto Rico post office, and only if the federal plant quarantine of Hawaii or Puerto Rico remains in effect.

274.923 **Terminal Inspections**

To implement the Terminal Inspection Act (7 U.S.C. 166), postal employees may cooperate with USDA and state agriculture personnel, provided that such cooperation is in strict accordance with pertinent provisions of section 274 and Publication 14, *Restrictions and Prohibitions on Mailing Animals, Plants and Related Matter.*

274.93 **Military Postal System**

This part does not apply to the military postal system overseas or to persons performing military postal duties overseas (see DMM E010).
274.94 **Customs Inspection in Territories and Possessions**

274.941 **American Samoa**
Pago Pago postal employees may permit designated American Samoa Customs officials, without a search warrant, to open, inspect, and read the contents of unsealed mail, and to examine the exterior (but not open or read the contents) of sealed mail that originates outside the Territory of American Samoa and is addressed for delivery within the Territory of American Samoa. Upon the request of American Samoa Customs officials, postal employees in the Pago Pago Post Office may ask the addressee of sealed mail that American Samoa Customs officials reasonably suspect contains dutiable or prohibited matter to authorize American Samoa Customs officials to open and inspect the contents of the sealed mail, or to appear at the post office to accept delivery of the sealed mail in the presence of an American Samoa Customs official.

274.942 **Guam**
Postal employees in the Agana Post Office may permit the designated Guam Customs officials, without a search warrant, to open, inspect, and read the contents of unsealed mail, and to examine the exterior (but not open or read the contents) of sealed mail that is addressed for delivery within the Territory of Guam. Upon the request of Guam Customs officials, postal employees in the Agana Post Office may ask the addressee of sealed mail, which Guam Customs officials reasonably suspect of containing dutiable or prohibited matter, to authorize Guam Customs personnel to open and inspect the contents of the sealed mail, or to appear at the post office to accept delivery of the sealed mail in the presence of a Guam Customs official.

274.943 **Northern Mariana Islands**
Postal employees in the Saipan Post Office and the Rota Post Office may permit designated Northern Mariana Islands Customs officials, without a search warrant, to open, inspect, and read the contents of unsealed mail, and to examine the exterior (but not open or read the contents) of sealed mail originating outside the Northern Mariana Islands and addressed for delivery within the Northern Mariana Islands. Upon the request of Northern Mariana Islands Customs officials, postal employees in the Saipan Post Office or the Rota Post Office may ask the addressee of sealed mail that Northern Mariana Islands Customs officials reasonably suspect of containing dutiable or prohibited matter to authorize Northern Mariana Islands Customs officials to open and inspect the contents of the sealed mail, or to appear at the post office to accept delivery of the sealed mail in the presence of a Northern Mariana Islands Customs official.

274.944 **U.S. Virgin Islands**
Postal employees in the U.S. Virgin Islands may permit designated personnel of the U.S. Customs Service, without a search warrant, to examine the exterior (but not open or read the contents) of sealed mail that originated in the CTUS and is addressed for delivery in the customs district of the U.S. Virgin Islands. Upon the request of such Customs personnel, postal employees in the U.S. Virgin Islands may ask the addressee of such sealed mail (which such Customs personnel have reasonable cause to believe
contains dutiable or prohibited matter) to authorize such Customs personnel to open and inspect the contents of the sealed mail, or to appear at the post office to accept delivery of the sealed mail in the presence of a Customs official.


Respectively, postal employees in any post office in the Commonwealth of Puerto Rico and the U.S. Virgin Islands are authorized to permit local excise tax officials to record for tax collection purposes the names and addresses that appear on the exterior of all incoming parcels that appear to contain taxable items, except those sent by registered mail. A postal employee must be present during such recording, and no mail may be opened, detained, or delayed for this purpose.

274.96 **Mail Addressed to Prisoners**

Authorized personnel of prisons, jails, or other correctional institutions, under rules and regulations promulgated by the institution, may open, examine, and censor mail sent from or addressed to, an inmate of the institution. An inmate may designate in writing an agent outside the institution to receive his or her mail, either through an authorized address of the agent, if the mail is so addressed, or at the delivery post office serving the institution, if the mail is addressed to the inmate at the institution.

275 **Physical ADP Security**

275.1 **General**


275.2 **ADP Contingency Planning**

275.21 **General**

All contingency planning must follow the unique needs of the organization using ADP equipment.

275.22 **Backup Principles**

Contingency planning should include reasonable consideration of the principles that follow:

a. If warranted, provide backup power to handle limited essential processing and support, such as air conditioning and humidification.

b. For extremely essential processing, provide equipment to monitor and adjust the voltage, current, etc., needed to maintain uninterrupted service.

c. Determine the location of computer installations that can provide backup processing for essential jobs, and negotiate mutual backup agreements.
d. Locate off-site storage for backup programs and data sets in a separate location beyond the immediate area of the data processing facility but near enough to be readily accessible in case of emergency. Records must be retrievable round-the-clock.

e. Consistent with the importance of the data and the cost of reconstruction, establish and follow a periodic (daily, every other day, weekly, etc.) backup schedule for files and programs, including transfer and updates, at the off-site storage facility.

275.23 Contingency Plans
All contingency plans, whether for natural disasters, man-made hazards, or work stoppages, must do the following:

a. Define essential processing functions to be performed in the event of partial or total shutdown of operations.

b. Contain specific individual assignments for each type of contingency.

Note: Do not include bargaining unit employees in a work stoppage plan.

c. Be distributed to all individuals named in the plan, reviewed at least every 6 months, and updated at least annually.

275.3 Periodic Reviews
In addition to periodic site visits by the Postal Inspection Service and/or the OIG, the management function responsible for the data processing site conducts its own review of security at least annually and maintains a written record of the results. Management reviews should be comprehensive and cover the guidelines in this section and any other current data protection guidelines.

276 Firearms Security
276.1 Issuance of Firearms
The issuance of service weapons and firearms authorizations is controlled by the chief postal inspector and inspector general and is limited to postal inspectors, special agents, and uniformed postal police officers.

276.2 Violations of Firearms Security

276.21 Having Firearms on Postal Property
Firearms on postal property — other than those legally mailed or those carried by authorized Postal Inspection Service and Inspector General personnel; by persons specifically authorized in writing by the chief postal inspector, inspector in charge, or inspector general; or by recognized law enforcement officers — are in violation of the rules and regulations for conduct on postal property (see the Postal Operations Manual; Poster 7, Rules and Regulations Governing Conduct on Postal Property; and Poster 158, Possession of Firearms and Other Dangerous Weapons on Postal Property Is Prohibited by Law).
276.22 Carriage of Firearms by Postal Employees
Postal employees carrying firearms while on official duty either on or off postal premises — other than those who are authorized by the chief postal inspector or by the inspector general — are in violation of the rules and regulations for the conduct of postal employees.

277 Identification Security

277.1 Purpose
Identification is issued for security control of access to postal premises and operations and to identify individuals as Postal Service employees. The Postal Inspection Service provides guidelines for all Postal Service identification programs.

277.2 Types of Accredited Identification

277.21 Headquarters Only

277.211 Top Officials
The following types of identification are issued exclusively by the deputy chief inspector, Operations Support Group, and are restricted to use by top postal management and distinguished official nonpostal visitors:

a. Board of Governors — A special white photo identification card issued to members of the Board of Governors over the signature of the chairman.

b. Form 128-B, Officer’s Identification Card (Green Card) — A special green photo identification card issued over the signature of the postmaster general to Postal Service officers.

c. Special Identification Card — A special white identification card, with expiration date, issued over the signature of the chief inspector. This card is issued to official nonpostal visitors such as members of Congress and Senate subcommittees.

277.212 Form 2041, USPS Building Pass — Headquarters
Form 2041 is a photo identification building pass for Headquarters employees issued and controlled by Human Resources.

277.213 Form 2041-A, Headquarters Building Pass — Tenant
Form 2041-A, a white photo identification card, is issued to nonpostal occupant employees and tenants at Headquarters. The holder’s employer’s name is entered on the face of the identification card. This identification is only honored at Headquarters.

277.22 Headquarters and Field

277.221 Form 128, Travel and Admittance Identification Credential Card (Blue)
Form 128, the blue and white photo identification card, is issued over the signature of the chief inspector or inspector in charge to executives and employees required to make frequent visits to postal field installations.
277.222 **Form 1823, EEO Credential**
Form 1823, *Equal Employment Opportunity Program*, a blue identification card, is issued over the signature of the vice president of Labor Relations, district manager, or inspector in charge to designated Equal Employment Opportunity (EEO) counselors, EEO counselors/investigators, or EEO investigators.

277.23 **Field Only**

277.231 **Form 1375, Employee Identification Card**
Form 1375, a blue identification card, is issued over the signature of the postmaster to employees at facilities where photo identification (Form 4098-F) is not in effect.

277.232 **Form 1375-P, Postmaster’s Identification Card**
Form 1375-P, a green photo identification card, is issued by district managers to all postmasters. The credentials remain valid until such time as a postmaster retires, resigns, is reassigned, or requires a new credential to replace one that is lost or worn out. Districts are responsible for the following:

a. Entering Social Security numbers in appropriate blocks.

b. Securing photographs and signatures to the forms and completing lamination of the credentials.

c. Issuing completed credentials to newly appointed postmasters.

d. Entering full name, title, office, state, and ZIP+4 above the signature of the district manager.

277.233 **Form 4098-F, Employee Identification**
Form 4098-F, a photo identification, is in use at larger postal facilities to provide visible identification of employees having a need to be on the workroom floor. Form 4098-F is issued and controlled by the postmaster to all employees at that facility, including letter carriers, special delivery messengers, and motor vehicle drivers. This identification must be displayed at all times while on duty inside the facility (see 277.3). While on duty away from the facility, letter carriers, special delivery messengers, and Motor Vehicle Service drivers must carry and display Form 4098-F when identification is needed.

277.234 **Item O8405A, Temporary Employee Badge**
Item O8405A is used in the following ways:

a. The control card portion is properly filled in by the issuing authority and kept in a card file at the installation. The badge portion is marked to indicate the areas to which the employee is authorized access. This is done by deleting those letters that designate areas where the employee is not authorized access. The expiration date is the next date after date of anticipated termination of the employee. On expiration, the control card and the returned badge portion are destroyed.

b. At larger installations where regular employees are required to wear the photo identification badge (Form 4098-F), the temporary employee badge may, at the discretion of the installation head, be issued in lieu of requiring the employee to return home to obtain a forgotten badge.
When a temporary employee badge is issued for this purpose, it is never validated for more than 1 day.

277.235 **Item O8405B, Visitor Access Control Badge**
The format of Item O8405B is similar to the format of Item O8405A (temporary employee badge) and it is completed, issued, and destroyed in the same manner.

277.236 **Item O8405C, Contractor Access Control Badge**
The format of Item O8405C is similar to the format of Item O8405A (temporary employee badge) and it is completed, issued, and destroyed in the same manner.

277.237 **Electromechanical Access Control Identification**
Electromechanical access control identification badges are identification badges procured locally that are needed to gain entrance to a postal facility where access is controlled by electromechanical means. These badges may have a photo identification placed adjacent to a Postal Service emblem on the front side. The reverse side has a statement of penalty for fraudulent use, and may also contain printed instructions indicating a return mailing address. An individual who is assigned this type of badge must surrender the badge on separation from the Postal Service.

277.24 **Highway Contract Route Contractor ID Cards**

277.241 **General**
Contractors, subcontractors, and their employees are issued accountable identification at the facility where they are employed. This identification must be worn in plain view at all times when the holder is on postal property.

277.242 **Form 5139, Nonpostal Service Temporary Employee**
Form 5139, an accountable yellow card with red lower and right borders, is issued to the above contract personnel for a period of 60 days while security screening is completed.

277.243 **Form 5140, Nonpostal Service Contractor Employee**
Form 5140, an accountable white photo identification card with red lower and right borders, is issued on completion of a favorable security screening.

277.25 **Postal Inspection Service**
The deputy chief for Operations Support Group controls the issuance of all postal inspector credentials and badges and special Postal Inspection Service credentials.

277.26 **Office of Inspector General**
The OIG controls the issuance of all OIG credentials, seals and badges. OIG credentials are issued over the signature of the inspector general.
277.3 **Displaying Identification**

277.31 **Proper Wearing**

All personnel assigned a Form 4098-F must wear it during official duty hours displayed on the outer garment over the left breast. When this is not practicable, Form 4098 is worn in plain view on the belt or as prescribed by the installation head. In addition, at installations where postal police officers are assigned access control functions, all employees are required to display their identification to the officer on entering the facility or grounds.

277.32 **Unauthorized Wearing**

Unauthorized possession of official identification or other insignia (Postal Service or imitations) is punishable by a fine of not more than $250 or imprisonment of not more than 6 months, or both. Employees wearing identification other than that issued to them are subject to disciplinary action.

277.33 **Special Situations**

Postal Service identification may not be worn in nonpostal employment or activities without authorization. The postmaster may authorize the wearing of Postal Service identification for activities in which the Postal Service participates or where identification with the Postal Service is beneficial.

277.4 **Requisitioning**

277.41 **Items**

The temporary employee, visitor access control, and contractor access control items (Items O8405A, O8405B, and O8405C) are available from both material distribution centers (see Publication 247, *Supply and Equipment Catalog*). Requisition of these items is restricted to information support field centers and districts, which may supply the items to smaller offices as needed. Generally these items should not be supplied to small offices where sight recognition is capable of providing the necessary identification. The material distribution centers furnish them as cost items in the following units of issue:

a. Temporary Employee Badge, packets of 50.

b. Visitor Access Control Badge, packets of 100.

c. Contractor Access Control Badge, packets of 50.

277.42 **Clips**

A reusable clip (Item O8404) used with the temporary employee, visitor access control, and contractor access control identification is stocked as a cost item at the South River Material Distribution Center. The clips are issued in packages of 50.
277.5 Custody and Protection

Protect identification or access badges by carefully controlling them. Keep supplies of unissued badges secure. Maintain a register that shows the employee’s name and title, date of issuance, date of return, and the number, if any, of the identification badge issued. Access control identification badges controlled by a computer must automatically record usage. The computer must also be capable of off-loading the recorded accesses to a device for storage that allows retrieval at a later date. Mutilate and destroy access badges that cannot be reissued or are unserviceable.

277.6 Returning Identification

All Postal Service identification is accountable property and must be surrendered when leaving the Postal Service or when a contract is terminated. Employees who are issued identification must return such at the time of separation or transfer.

277.7 Lost or Unreturned Identification

277.71 Precautions

Take every precaution to prevent identification from falling into the hands of unauthorized persons. Employees must immediately report to their supervisors a lost or unserviceable identification. Report recovered identification promptly.

277.72 Replacement Fee

Charge $1 for each replacement of a lost identification or for failure to return such on separation. This does not apply to Christmas or other temporary employees.

28 Emergency Preparedness

281 Contingency Planning

Each federal department and agency, including the Postal Service, is responsible for the development of plans for actions necessary to maintain itself as a viable part of the federal government during any emergency that might occur. Preparedness planning within the Postal Service ranges from domestic emergencies, such as conditions resulting from natural or human-caused disasters, to international emergencies, including nuclear war. These conditions may affect a single postal facility or have a widespread effect on the entire Postal Service.
**Authorities**

The Postal Service derives authority for participating in emergency preparedness programs primarily from the following:

a. Title 39 U.S.C.

b. Executive Order 12656, dated November 18, 1988, which combines the assigned emergency functions of all federal agencies into one document. Parts 1, 2, and 26 of the executive order pertain to the Postal Service.

---

**Preparedness Planning Objectives**

The primary objective of postal emergency preparedness planning is to maintain or restore essential postal service in a national emergency, natural disaster, or disruptive domestic crisis. Details of Postal Service preparedness plans can be found in the following documents:

a. Publication 159 series on contingency planning (A through D).

b. ASM 28.


d. ELM 519.22 and 519.23.

---

**Planning Responsibilities**

**284.1 Postal Service Emergency Coordinator**

The chief inspector is the emergency coordinator for the Postal Service. The emergency coordinator receives authority directly from the postmaster general and is responsible for coordinating emergency planning and civil preparedness programs applicable to all elements of the Postal Service.

**284.2 Vice President, Area Operations**

Vice presidents of Area Operations are responsible for developing, directing, and operating all emergency mail service and related activities in their respective areas and districts under guidelines issued by Headquarters. The vice president of Area Operations may designate a staff member as the area emergency coordinator to directly supervise the overall emergency preparedness planning activities under the manager’s jurisdiction. The emergency coordinator works closely with district managers and the inspectors in charge in the development of integrated plans to provide emergency mail service and related activities for the area during emergency situations.

**284.3 Emergency Coordinating Committees**

**284.31 Headquarters**

An emergency coordinating committee is established at Headquarters and consists of primary and alternate members from each operating element (see Headquarters Circular 80-10, *USPS Emergency Coordinator; Civil Defense*...
Coordinator, and Headquarters Emergency Coordinating Committee). The Headquarters committee assists the Postal Service emergency coordinator or others, as appropriate, to develop and implement emergency preparedness plans for Postal Service Headquarters and to prepare guidelines for use by the inspector in charge and vice president of Area Operations to develop emergency preparedness plans. The Postal Service emergency coordinator or designated alternate chairs this committee.

284.32 Area Office

An emergency coordinating committee is established in each area office (see Management Instruction AS-280-89-6, Coordinator of Regional Emergency Preparedness Planning). The area office emergency coordinating committee assists the inspectors in charge and district managers, as appropriate, in developing and implementing emergency preparedness plans consistent with guidelines issued by Headquarters.

284.4 Postmasters

Postmasters do the following:

a. Carry out emergency preparedness assignments, programs, etc., as directed by the vice president of Area Operations.

b. Comply with and cooperate in community civil preparedness plans (including exercises) for evacuation, “take cover,” and other survival measures prescribed for local populations.

c. Designate representatives for continuing liaison with local civil preparedness organizations, if such activity does not interfere with normal duties.

d. Volunteer to serve (at their own option) as members on the staff of the local state emergency management office, if such service does not interfere with their primary postal responsibility in an emergency.

e. Authorize and encourage their employees to participate voluntarily in nonpostal pre-emergency training programs and exercises in cooperation with states and localities.

285 Contingency Plans

285.1 Domestic Emergencies

285.11 Examples

Examples of domestic emergencies are:

a. Natural disasters.

b. Strikes and work stoppages by postal employees.

c. Strikes by nonpostal labor organizations.

d. Civil disturbances.

e. Bombs and bomb threats.
f. Fires.
g. Accidents involving mail-carrying planes, trains, or highway contract vehicles.

285.12 **Guidelines**
Contingency planning guidelines for maintaining continuity in the Postal Service during domestic emergencies are contained primarily in parts A, B, C, and D of the Publication 159 series on contingency planning. Also see the ELM and the *United States Postal Service Emergency Planning Manual.*

285.13 **Developing Plans**

285.131 **Contingencies**
Each management level throughout the Postal Service develops contingency plans under the Publication 159 series to provide emergency postal services.

285.132 **Advance Information**
The plans must include procedures for providing as much information as possible on potential or actual emergency situations and their possible adverse impact on postal operations. This provision of information includes disseminating advance warnings, suggesting precautionary protective measures, and ensuring that all emergency equipment on hand is in working condition, and that its operation is understood by all personnel concerned.

285.2 **International Emergencies**

285.21 **Definition**
*International emergencies* are conditions resulting from worsening international relations, wartime mobilization activities, or an attack on the United States, including a nuclear attack.

285.22 **Guidelines**
Guidelines for preparing and maintaining plans to ensure continuity of postal operations during international emergencies are in the *United States Postal Service Emergency Planning Manual* (EPM), the basic planning document for the entire Postal Service. It provides the emergency standby guidelines and specifies essential post attack functions of the Postal Service, with instructions and procedures. Also see the *Employee and Labor Relations Manual* (ELM).

285.23 **Developing Plans**
Each Postal Service management level develops and maintains an emergency preparedness plan following its vice president’s guidelines and developed from instructions in the EPM.

285.3 **ADP Contingency Plans**
286 Emergency Lines of Succession

286.1 Postmaster General
In case the postmaster general is incapacitated from an enemy attack or other national emergency, the following is the line of succession to perform the duties of the postmaster general (see 112.11):

a. Deputy postmaster general.
b. Chief operating officer and executive vice president.

286.2 Headquarters and Field
Each corporate Headquarters unit and Headquarters field unit establishes its own internal line of succession to provide for continuity under emergency conditions. Vice presidents, district managers, plant managers, inspectors in charge, and postmasters or officers in charge of other field installations, as specified in the EPM, prepare a succession list of officials who are to act in their stead if they are incapacitated or absent in an emergency. Show orders of succession by position titles.