Contingency planning

Explosive devices in the post

UPU Postal Security Group

Berne, December 2021

Nes

Table of contents Page

Foreword

This document is provided by the Universal Postal Union to assist postal facility managers and supervisors in dealing with bomb threats, explosive devices in the mail and other situations that could endanger life or property. The document provides guidelines and recommendations for postal officials in the development and maintenance of facility contingency plans addressing explosive devices and bomb threats.

Security accepts no compromises. Accurate assessment of security risks and implementation of preventative measures are the only way to protect postal service staff and customers effectively.

1 Introduction

Criminal and terrorist acts include threatened and actual bombings of commercial and government facilities and individuals. Despite the range of variables between a threat and an actual bombing, we must never lose sight of our basic objective: to ensure the safety of all postal personnel, as well as customers and visitors on postal premises. It must be stressed, however, that the manner of constructing an explosive or incendiary device is limited only by the ingenuity of its maker, and no procedure can guarantee safety in all situations.

2 Scope of the guidelines

These guidelines are necessarily broad in scope because of the different sizes of postal facilities and the wide range of possible situations that may occur. They are intended to aid in the preparation of local contingency plans and should be adapted to individual facility requirements, including airport mail facilities.

3 Responsibilities

3.1 Director of the facility

In the event of an explosion, the identification of an explosive device or credible bomb threat, the director of the facility will serve as the incident commander. As such, they will make initial decisions on proper response and must therefore be directly and immediately informed in case of a critical incident. Additionally, they will make sure that proper procedures and measures against explosive devices and bomb threats are implemented. The director will usually designate a suitable manager as installation head; the latter will maintain continuous contact in case of an incident. The director ultimately retains responsibility for compliance and planning.

3.2 Installation head

The installation head in a postal facility must furnish the leadership and guidance necessary to plan for and deal with bomb threats, explosive devices and explosions. The installation head is expected to exercise judgement in evaluating the facts and developing and implementing responses. Responsibilities include:

- developing a bomb threat assessment process and contingency plan, keeping in mind all facilities and personnel that could potentially be affected;
- defining roles and responsibilities for those assigned to respond;
- setting up critical incident teams;
- instructing personnel on proper bomb threat response;
- training supervisors tasked with ordering evacuations;
- depending on the local rules, designating search teams;
- briefing shift supervisors;
- dealing with the media;
- coordinating critical incident response and communication with outside responders, e.g. postal security, police, explosive disposal officers, airport authorities;
- preparing plans (i.e. various degrees of response) to strengthen facility security in the event of a bomb threat.

The installation head should have extensive knowledge regarding the security of the facility and have received training on critical incident response.

To ensure roles and responsibilities are effectively assigned in the event of a critical incident, all relevant parties, especially the police, should be involved from the beginning.

3.3 Postal security

Designated operators should train at least two senior postal security officers (who can be contacted 24 hours a day) to assess threats and risks.

Postal security officers should be trained to recognize information patterns that can assist with accurate threat assessment.

3.3.1 Postal security officers

Postal security officers (may also be called: inspectors, security specialists, security managers or investigators) are responsible for leading and/or coordinating with other agencies the investigation of bomb threats and explosive devices found in the mail, in postal facilities or on postal property, including postal vehicles. Assistance from outside agencies should be requested when needed.

Specific responsibilities and roles must be described in the contingency plan, particularly regarding searches, evacuation, crime scene integrity and preservation of evidence.

If they are at the scene, postal security officers have primary responsibility for dealing with bomb threats and explosive devices in the mail, in postal facilities or on postal property until the police or another appropriate authority arrives. Postal security officers should advise on emergency procedures and on which services to contact. As an incident or threat continues, they should coordinate the response with all emergency services. If they are not at the scene, emergency procedures must nevertheless be implemented prior to their arrival.

Throughout the incident and immediately following, postal security officers should brief the installation head and/or director of the facility on the situation.

3.3.2 Postal security force

Some designated operators have established a postal security force (in addition to the “traditional” investigation service). Postal security force personnel are assigned specific roles and responsibilities under the contingency plan, particularly for searches, evacuations, crime scene integrity and evidence.

3.3.3 Inspector in charge/security expert/chief security officer

This official is responsible for the overall supervision and administration of postal security officers/inspectors/security specialists/security managers/investigators and – if established – the postal security force.

3.4 Other employees

Personnel other than installation heads and security staff must report threats immediately to pre-designated supervisors, who ensure that the proper authorities are notified.

3.5 Police

The local police department is the first and most important outside agency brought in to deal with a critical incident involving an explosion, explosive device or bomb threat. Usually the local police department will respond immediately and inform the local bomb squad as well. Depending on the local emergency plan, the police will also notify other emergency teams (fire department, emergency medical services, etc.).

3.6 Fire department

In the event of an explosion or bomb threat, the fire department must be contacted. In addition to extinguishing fires, the fire department can aid in handling hazardous, toxic or other dangerous substances. The fire department may also determine whether a facility needs to be evacuated.

3.7 Medical services

If there are any signs or symptoms of injury or illness, medical services must be contacted.

3.8 Airport authorities

Postal facilities located at or near an airport must inform the airport authorities in the event of a critical incident. Often airport authorities have procedures for responding to critical incidents, including coordination with other emergency teams.

4 Advance planning

4.1 Background information

A number of aspects must be considered and questions answered in preparing an emergency operations plan.

4.1.1 What are you looking for?

Improvised explosive devices (IEDs)

– IEDs can range from victim-activated explosive devices, to timed devices, to command-detonated devices. Explosive devices in the mail can range from small victim-activated letters to parcels containing IEDs that could potentially bring down an aircraft.

– IEDs can consist of everyday objects prepared with a certain amount of explosive material.[1]

Improvised incendiary devices (IIDs)[2]

– IIDs are defined as any material, substance, device or combination thereof which is capable of supplying the initial ignition and/or fuel for a fire.

– IIDs can range in size and can be contained in something as small as an envelope.

– They can be made from everyday objects prepared with an incendiary material.

IEDs and IIDs sent by post are typically designed to:

– harm the recipient (victim-activated);

– sabotage the transport vehicle (truck, plane, boat, etc.);

– disrupt a post office, airport, handling agent's premises or mailroom;

– harm the staff handling the item (although this is a rare occurrence).

4.1.2 When should you look for IEDs/IIDs?

– On a regular basis, by having postal staff visually profile items during the normal sorting process.

– Following receipt of a threat (by telephone or in writing). Such threats are a common technique used by:

  - professional terrorists;
  - disgruntled employees (former or current);
  - mentally unstable persons;
  - children (pranks, school holidays);
  - competitors/business rivals;
  - special interest groups with known radical or violent tendencies, e.g. animal rights groups, religious protesters, anti-abortion activists, neo-Nazi groups, etc.

[1] Explosives are characterized as "high" or "low". Materials that detonate are said to be "high" explosives (e.g. TNT, dynamite), and materials that deflagrate are said to be "low" explosives (e.g. black powder, smokeless powder). Explosives may also be categorized by their sensitivity. Sensitive materials that can be initiated by a small stimulus of friction, impact, shock, heat or electrostatic charge are considered "primary" explosives, and materials that are less sensitive are "secondary" or "tertiary" explosives. Homemade explosives (HMEs), namely, commercially available ingredients combined to create an explosive substance, are becoming more common owing to the ease of information sharing.

[2] When mixed or ignited, incendiary materials will burn ferociously.

– Following receipt of information from an intelligence agency, the police, other postal operators, civil aviation authorities, the UPU Postal Security Group, INTERPOL, etc.

– Following an incident (activation of an explosive/incendiary device at the point of delivery or in transit).

– When a suspicious package (that has not detonated) is found in transit.

4.2 Risk and threat assessment

Designated operators should establish procedures to assess threats received and the risks posed by the situations described in 4.1. The main objective is to protect employees, public property and mail with minimal cost and disruption.

4.2.1 Risk

What is the potential for loss of:

– life?

– property?

– equipment?

– mail processing time?

4.2.2 Threat

– What level? High, moderate, low?

– Specific to one area, building, group or person?

– Does the general threat affect many buildings or many groups?

4.2.3 Threat and risk assessment combined

It is important to note that it is possible to:

– have a **high threat** assessment but a **low risk** assessment. In this case, the security officer may decide to apply limited or no additional security measures, depending on the circumstances at the time.

– have a **low threat** assessment but a **high risk** assessment. In this case, the security officer may decide to apply additional security measures.

In order to make an accurate threat assessment, it is vital to have as much information as possible. All threats should be reported immediately, and the decision-making process should be documented and retained.

The threat assessment will dictate what procedures will be required.

If there are specific indications ruling out the seriousness of the threatening call → Concentrate on ascertaining who the perpetrator is and exclude further measures.

If there are doubts about the seriousness of a bomb threat, but they cannot be clearly proven → Order a preemptive search of the site of the threat *before* or, if reasonable, without evacuation.

If the threat is credible → Establish escape routes, obtain information about head counts, order evacuation, perform a targeted search.

The threat/risk assessment can result in one of three levels of response:

No Target Identified	No extra precautions required. Resolve any deficiencies identified in the security process
Limited Response Required	Set up additional security processes/checks as soon as possible. Set a time limit for additional security measures at which point the threat should be reviewed and reassessed, e.g. daily, weekly or monthly
Immediate Response Required	Respond immediately with additional security measures specific to the threat. Review/assess the threat/risk to other corporate divisions. Set a time limit for additional security measures at which point the threat should be reviewed and reassessed

4.3 Developing a bomb threat contingency plan with senior staff

All postal facilities, including postal data centres, airport mail centres, mailbag depositories, agencies and branches, must have a bomb threat contingency plan.

Prepare plans (i.e. various degrees of response) to strengthen facility security in the event of a bomb threat.

As manager, you should review these guidelines with members of your senior staff and with postal security officers.

Contingency plans should be circulated to all levels of management and appropriate training should be arranged.

In all of the above cases, input should be sought from police, intelligence services and other professional security organizations where it is prudent to do so. Planning with outside agencies will lead to a better coordinated response in a critical incident.

/ Prepare a telephone and contact list (see example in Appendix C).

4.4 Evacuation planning

As manager, you should review these guidelines with members of your senior staff and with all station and branch superintendents. In establishing an evacuation plan, pay particular attention to the priority of routes of evacuation, based on building design and location of personnel within the building.

The plan should include the following:

– Design plan of the different areas and floors of the building, identifying the official escape routes. Parts of this plan should be posted in all significant areas of the building.

– Contact list of supervisors responsible for evacuation of specific areas of the building.

– Designated meeting point at a *safe distance from the building* for evacuated staff. Remember that based on some threat assessments it *may be safer* to keep staff in the building, e.g. in the basement. This scenario should be planned well in advance and advice sought from the constructors of the building as well as from explosive experts. Keep in mind that a coordinated attack may include secondary devices placed at an obvious meeting point.

– Security protection plan for all fixed credits, accountable mail, etc.

The following aspects should also be considered for planning purposes:

– The size of the building, number of occupants or users, type of use and location.

– Whether the threat concerns a suspicious item that was placed in a specific location or an item in the mail. Was it transported with the mail or found near a postal facility (e.g. a briefcase left in a stairwell)?

– Whether the threat is assessed as valid. This is based on the information available and the advice of postal security management and the police.

– Whether an explosive device is discovered during a search.

Supervisors who have the authority to order evacuations should be well trained on evacuation response. This includes:

– searching the entire escape route, including the staircases, before the evacuation;

– determining which personnel will be directed to particular routes;

– ensuring elevators are not used.

Advice on evacuation training techniques is usually available from the police, fire department or other municipal services.

4.4.1 Assuming authority for evacuations

It is your responsibility as manager to protect the safety and lives of people in the building under threat in all circumstances. It is generally safest to evacuate the whole building or all the affected areas. Nevertheless, based on sound judgment and experience, you may decide not to evacuate. A hasty evacuation could endanger more lives through panic than an actual explosion.

4.4.2 Re-entering the building

It is often the facility manager who makes the decisions to evacuate and re-enter the building. The security staff should be allowed to return first, so that they can re-secure the premises and reinstate access control measures. Evacuation and re-entry decisions should follow the advice of the postal security officers, local police or other competent authorities.

5 Selecting a holding area for suspicious items

A non-mail item suspected of being an explosive device discovered on postal service property should never be touched or moved until thoroughly examined and determined to be safe by the responding bomb squad or postal investigators.

In advance, designate one or more areas where a suspicious item can be taken by the bomb disposal unit to be examined or disposed of without endangering staff, buildings or equipment. This may be a location behind the building or other isolated area, parking lot, etc. The best route to the holding area from various locations within the building should be mapped out during the planning stage.

N.B. – Finding an isolated area at an airport may be a problem. A specially designed containment area may be required.

6 Bomb threat search teams

In planning for bomb search and discovery, appoint the search teams (at least two people each) and assign each team a specific area to search. At least one member of the search team should ideally work in the assigned area or, at the very least, be familiar with it. The teams should consist of volunteer employees identified in advance, managers, supervisors and postal security officers. It is essential that each team member understand the assignment and respond promptly when called upon. Time and thoroughness are of the essence.

7 Training and preparing the search team

The number of sections of the building to be searched and which items are particularly suspicious must be determined locally. Search team members must be thoroughly familiar with all hallways, restrooms and cisterns, stairwells, false ceiling areas, ventilation shafts, and every other conceivable location in the building where an explosive or incendiary device could be concealed. The search teams must be thoroughly trained and familiar with the floor plan of the building and immediate outside areas. The training must also cover:

– communication with the individual in charge of the search (control centre);

– evacuation orders if a suspected explosive device is found;

– escape routes.

Training in search techniques may be provided by the police, fire department, armed forces or other municipal services.

Team members should be equipped with flashlights. Arrangements should be made for search teams to have access to keys to all areas of the building during an emergency. A rapid two-way communication system should be established, possibly through the use of existing telephones. Caution: The use of two-way radios and mobile phones during the search can be dangerous. Radio signals may trigger an electronic detonating device.

8 Searching for explosive devices

Basic principles of a search in response to a bomb threat:

– The initial search area may be determined according to the details provided in the threat.

– Never search alone; maintain contact with people overseeing the operation.

– Each search team should consist of at least two people.

– Avoid using radio devices and mobile phones (risk of triggering detonation).

– Each area should be searched twice by different search teams.

– Establish primary and alternative evacuation routes. Select evacuation routes and assembly areas that are not in the vicinity of the suspicious item(s). Ensure that the routes have been searched and cleared.

– Other indoor areas are not searched until all public areas on all floors have been searched.

– Areas that have been searched should be identified with a specific marker.

When the location of a possible explosive device is unknown:

– Start from the outside of the building and work your way in.

– Check storm gutters, window ledges, bushes, trees, platforms and garbage bins adjacent to the building.

– Begin the search of the interior with areas accessible to the public (hallways, restrooms, lobbies, stair-wells, elevator shafts, telephone booths, fire hose racks, ceiling lights, souvenir stands, closet areas, boardrooms and any other likely targets of an attack).

– Always search from the bottom (basement) to the top (including the roof).

– Remember that it is important to move swiftly, but not to the detriment of a thorough search.

Consider using outside resources. An explosive detection canine could be extremely useful in performing the search.

9 Explosive device search and discovery – do’s and don’ts

Do:

– keep in mind that more than one explosive device may be planted;

– complete the search as rapidly as possible.

Do not:

– engage in horseplay while searching;

– become careless or overconfident;

– permit smoking in the immediate vicinity of a suspected explosive device;

– allow two-way radio or mobile phone transmission near a suspected explosive device, as this could trigger detonation;

– assume identification markings on any suspected explosive device are legitimate;
– touch any object attached to a suspicious item as this could be a pressure release device;
– submerge a suspicious item in water as this can trigger electric circuits and violent reactions with chemical agents;
– shake or jar a suspicious item as this may cause certain chemicals to mix, triggering an explosion or violent reaction.

10 Removal or disarming

It is imperative that the members of the search team understand that their mission is only to search for reported suspicious items. Under no circumstances should they touch, move or shake a suspicious item or anything attached to it. The removal or rendering safe of the device must be left to professional disposal units.

11 If a suspicious item is discovered

General principle: time, distance and shielding are key to safety

– Isolate the suspicious item without disturbing it in any way.
– Before evacuating the danger area, search the escape route.
– Evacuate the danger area or the entire building as appropriate or as instructed by law enforcement personnel.
– In evacuations owing to IED threats, if windows and doors are open, leave them open to minimize damage in the event of an explosion. (The normal procedure in case of fire, i.e. IID threats, is to *close* all doors and windows). Evacuated employees should be instructed to stand clear of open doors and windows.
– After the building has been evacuated, re-entry must not be authorized until a search has been completed and any suspicious item has been removed or declared safe by the police.

12 Security measures for suspicious items found during mail processing

When dealing with a suspicious item in the mail, remember that if it contains an explosive or incendiary device, it is likely designed to activate when the item is opened or the contents removed (victim-activated). As the item has probably been handled numerous times and transported from afar, it should only become dangerous if opened or handled incorrectly. The following precautions should be taken when handling a suspicious mail item.

Do not:

– try to open the package or envelope;
– pass the item to another person for a double check;
– bend the item;
– tear the item or move it excessively;
– place the item near heating appliances;
– place the item in water or in a humid room;
– cover the item;
– keep the item with other mail items.

Do:

– evacuate the area;

– alert your manager;

– alert the postal security officer;

– follow instructions;

– follow the contingency plan for your facility.

/ (See Appendix D – Security procedures for suspicious items)

13 Dealing with the media

The media often ask detailed, probing questions. In their haste to defend the organization's reputation, management and staff may inadvertently release details of the security countermeasures in place at the time of the incident. This can undermine the security regime and result in additional security measures at extra cost. *If possible, avoid contact with the media.* If media attention cannot be avoided, coordinate the release of information (as little as possible about security countermeasures) with postal security officials and the public relations department.

14 Threats to multi-tenanted buildings

In buildings that postal operators share with other tenants, all parties should work together to develop a contingency plan for the entire building. The plan should specify who has the final say on the evacuation of each area and what the evacuation routes are.

15 Briefing shift supervisors

All supervisors on each shift and in each work area must be familiar with and understand the contingency plan for their facility.

They must have immediate access to the names and telephone numbers of the appropriate emergency units, i.e. security control officer, postal security officer, police, and military explosive ordnance disposal units or other bomb disposal squads, as required by the contingency plan.

16 Strengthening facility security

At a minimum, the following preventative measures to strengthen facility security should be taken:

– Establish and strictly enforce procedures for controlling access to work areas. Ensure that unauthorized people do not have access to work areas.

– Ensure that doors and access points to areas such as boiler rooms, computer rooms, switchboards, elevator controls, janitor closets, etc., are securely locked when not in use.

– Instruct all personnel to look out for suspicious people and activity.

– Instruct all personnel to report the location and provide an accurate description of suspicious items or parcels seen on or near postal property.

– Ensure that fire exits are not obstructed.

17 Strengthening the postal security process – screening methods

Postal security officers/managers have a number of security screening measures available to them. These measures include:

– profiling;

– manual search;

– vapour detection;

– metal detectors;

– explosive detection sprays;

– X-rays.

N.B. – Reference to “screening” is often understood as X-ray screening. However, there are many different types of screening. Common and clear language must be used so that the security officer knows exactly what is meant when someone suggests “screening” the mail or claims to have “screened” the mail.

17.1 Profiling

All items of mail, large and small, should be inspected (profiled) during the normal sorting process by postal staff. Staff should be trained to look for the following:

– Markings that restrict the group of recipients, such as “confidential” or “personal”.

– Addresses that are typed, poorly handwritten, cut and pasted or composed of a montage of individual letters.

– Incomplete addresses (no name), made out to the head of a department.

– Items sent to high-profile or high-risk companies/persons, members of the government or public figures:

  - Potential targets are very diverse and can range from the general public to sports personalities, celebrities or members of the government. It would be impossible to prepare a list of potential targets for the profiling staff to use.

  - If profiling is to be effective, the staff conducting the profiling must be briefed on *potential* threats in their delivery area (by the shift manager as required, i.e. daily, weekly, monthly or when a threat has been declared). Staff should be made aware of known potential targets.

  - Managers in particular should be aware of the potential targets in their delivery area in case an employee identifies a suspicious item. Profiling combined with knowledge about potential targets enables the responsible manager to make a sound risk assessment.

  - Recently, incendiary or explosive devices have been sent to members of the public following a disagreement or argument between friends, relatives, spouses, colleagues, etc. These names will not arouse any suspicion as the individuals are not high-profile figures. If an item has suspicious characteristics but the address does not raise suspicion, *do not automatically dismiss it as safe.*

– Generic or fictitious return address or no return address.

– Excessive wrapping, heavily taped or glued seams.

– Excessive postage. Often more stamps than necessary for the weight/destination are used to avoid weighing of the item at a post office counter.

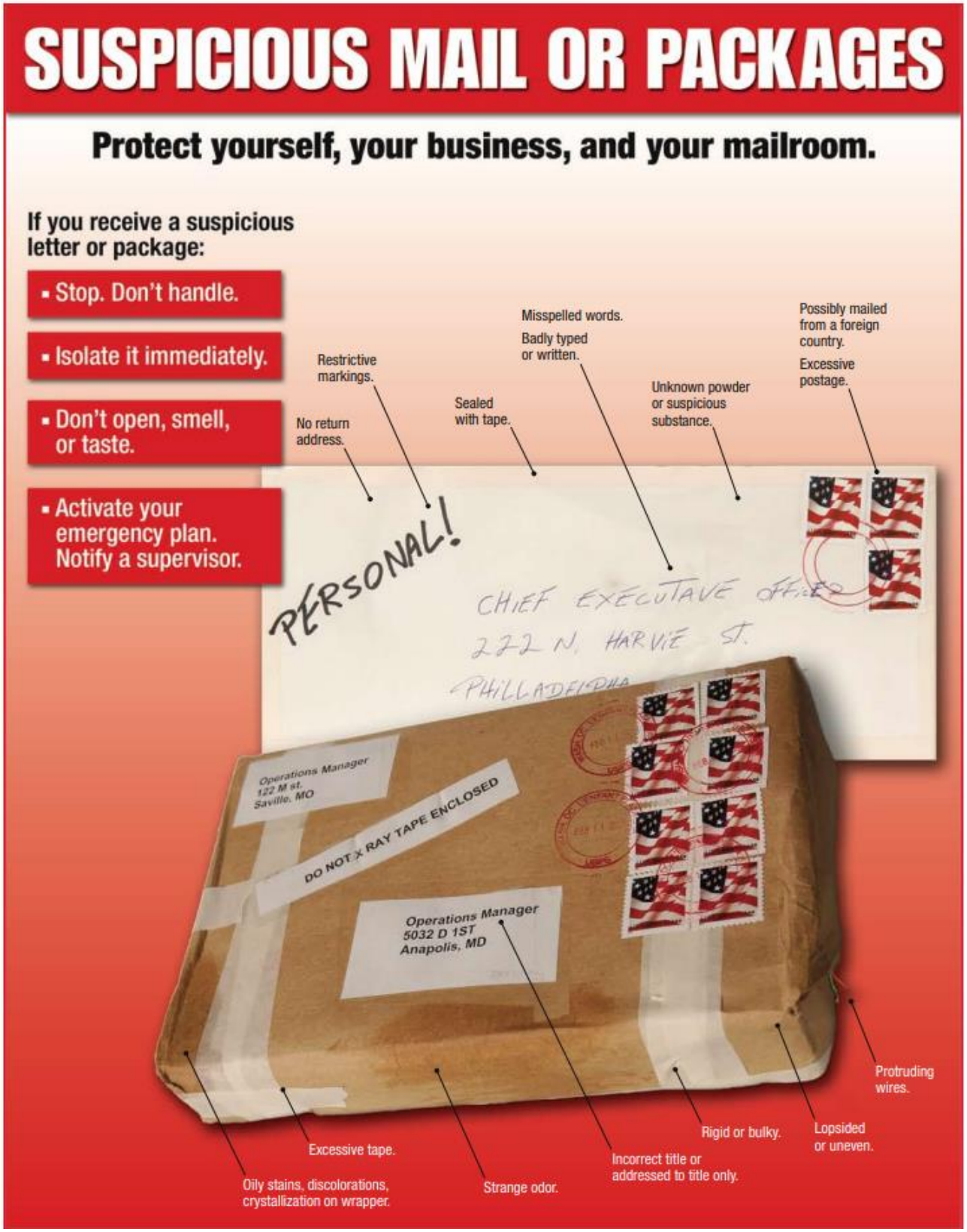
– Heavy/uneven weight distribution. An unbalanced item could contain loose articles, powder or liquids.

– Stiffness. A stiff material may be placed in the package to prevent the IID/IED from breaking apart in transit. *(Do not bend* suspicious packages.) One method of concealing mail bombs is in a book. A book provides a protective covering and is sturdy enough to support the device.

– Protruding wires or foil or pin holes in the wrapping (used to arm or activate the device).

– Grease marks. Some explosives leave a residual greasy stain on the packaging paper.

– Other suspicious signs.



Staff should be made aware of any current threat information that may help with the identification of IEDs or IIDs in the mail.

/ (See Appendix E – Profiling list)

17.2 Manual search

Manual searches are:

– often prohibited (mail is protected by law and packages can only be opened under certain very specific conditions);

– very slow;

– impractical if the item is an electrical appliance, e.g. a radio (the back would need to be removed to inspect the inside);

– dangerous when dealing with a victim-activated device.

17.3 Vapour detection

The following are available to detect explosives using the vapour method:

– Dogs/pigs
  - Both are very effective for detecting all types of explosives, provided they have been properly trained and are re-trained regularly.
  - Short attention span, can only work for limited periods before they require a rest period. Not always ideal in an office environment.

– Vapour detectors
  - Equipment that detects vapour from explosive material (most effective on nitroglycerin- based explosives).
  - Not all explosives emit detectable amounts of vapour. Additionally, mail requires vapours to be detected through the packaging, which may prove difficult for the average detector. If the detector fails to detect small quantities of vapour, it could result in an “all clear” signal even though the threat still exists. The limitations of this equipment should be recognized by those using it.

– Vapour/particle detectors
  - Equipment that detects vapour and particles from explosives.
  - Not all explosives can currently be detected using this type of equipment.
  - Particle detectors look for contamination of the outer packaging.
  - There may be insufficient particles/material for the machine to detect explosive materials.
  - This equipment requires a very precise sampling technique.
  - The sampling and analysis process is time-consuming.

17.4 Metal detectors

As the name suggests, this equipment detects metal. Working on the assumption that a normal package or letter will contain no more metal than that contained in a few paper clips or staples, the metal detector will go off when it detects slightly larger metal objects, such as batteries, wire, foil or a timing device, which are common components of a functional explosive device.

In theory, this screening method is fast, efficient and effective; however, in practice, the result only indicates that the item being screened contains metal. The signal will still need to be interpreted, i.e. louder = more metal, quieter = less metal. Deciding whether the item is a threat based only on interpretation of the alarm signal can easily lead to the wrong determination. At best, the metallic item would prove innocent; at worst the item could be triggered when opened. Screening with metal detectors should only be performed by trained staff and all positive results treated with caution.

17.5 Explosive detection sprays

Two types of explosive detection sprays are:

– sprays that make the paper semi-transparent;

– chemical reagent sprays (chemicals react to traces of explosive by changing colour).

Both types of sprays have limited use in explosive detection. In fact, they can cause more problems than they solve:

– storage problems (toxicity);

– protective clothing and/or breathing apparatus required for staff using the sprays;

– the amount of explosive required to trigger a colour change is quite high;

– explosive devices may be triggered by light, so rendering paper packaging transparent with the spray could cause problems;

– if the package turns out to be non-hazardous, the sprays could damage the contents.

17.6 X-rays

X-rays are one of the most effective ways of screening for IEDs and IIDs in mail items; however, a number of different devices and techniques can be used. If your security officer has been advised by a third party that the mail has been x-rayed, you should ask more detailed questions. The answers to the following questions should be reviewed very carefully, as they could affect your risk assessment.

– What type of X-ray system was used?

– Was the mail screened in bulk (e.g. in large aircraft containers, large mailbags or pallets)? It is more difficult to detect small threat items by X-ray if they are concealed within larger masses.

– Was the mail screened in small amounts, e.g. in trays or small bags as opposed to large bags (to increase the ability to detect dangerous items)?

– Were the screeners operating the X-ray trained/certified to identify explosive devices?

When deciding what security measures to put into place, the security officer should be aware that more than one security measure can be implemented at one time, e.g. profiling and X-ray or vapour detection. The benefits gained by using multiple screening methods include enhanced detection capabilities and more opportunity to eliminate non-hazardous items.

18 Initial response to a bomb threat

18.1 Receiving bomb threats – in person or from another party

Bomb threats are sometimes received in person by counter clerks, supervisors, elevator operators or other individuals. Notifications of bomb threats or similar acts may also be relayed through newspapers, radio stations, police stations, authorities or other sources.

All staff must report threats *immediately* to the relevant supervisors or directly to the security office. Postal security officers, facility management, the police, appropriate area or district officials, and airport and airline managers will then be alerted as required.

18.2 Calling the explosive ordnance disposal or bomb squad unit

In many countries, the police have specially trained and equipped bomb disposal units. If the local police department is unable to dispose of an explosive device, the military may be of assistance.

The specific unit to call in an emergency must be determined in advance.

The security control officer, with assistance from the police and other security organizations, assesses the threat and decides whether to contact an explosive ordnance disposal unit.

18.3 Notifying other authorities

If the threat applies to an airline or a specific flight, it must be reported immediately to airport and aviation authorities. Every courtesy is extended to airport authorities and inspectors in the safeguarding of lives and property and for the handling of mail that is on a plane or in an airline's custody during a bomb threat.

18.4 Other measures

If there is reason to believe that a particular piece of mail is suspicious, isolate it in a holding area pending its examination by an expert. Try to limit handling the suspicious item as much as possible. Hold other mail until it is released by the appropriate authorities.

19 Responding to telephone threats

All personnel who normally receive telephone calls from the public should be briefed on explosive devices and bomb threats. They should comply with the proper telephone procedures and follow the bomb threat response guidelines outlined above.

To assist employees in obtaining as much information as possible and to establish uniform reporting procedures, keep a checklist near each telephone used for incoming calls from the public.

/ (See Appendix F – Example of a telephone bomb threat report)

If a caller makes a bomb threat, staff should:

– Covertly raise the alarm with a colleague.

– Keep the caller on the line as long as possible (potentially allowing time for the call to be traced).

– Ask the caller's name (bombers may be seeking media attention for their actions or may give their name inadvertently. In any case, a name provides additional information for the security officer.)

– Ask the caller to repeat the message (to make sure you have understood everything properly).

– If possible, write down every word spoken by the person making the call (it is vitally important to write down the exact words used. The text may contain a code word or clues to identify the person threatening the facility.)

– Ask the caller to provide the location of the device and the time of possible detonation.

– Inform the caller that the building is occupied and that an explosion could result in death or serious injury to many innocent people.

– Listen for strange or peculiar background noises, such as engines running, background music or any other noises that might provide clues to where the caller is.

– Note whether the voice is male or female.

– Listen for distinctive speech patterns or accents.

– Activate call tracing immediately if available.

– Record the time the call was received and terminated (noting which timepiece was used to record the time, as it may be fast or slow).

Immediately after the caller hangs up, the staff member should report all gathered information to the person designated by the facility manager and write a brief report detailing the episode.

The employee who received the call should not discuss the threat with their colleagues. Discussing the call with another colleague could cause the facts of the call to become confused. Additionally, the information could cause panic among some staff members.

20 Responding to an incident

If an explosive device is triggered, the facility manager should do the following:

– Promptly evacuate the whole building or the relevant areas.

– Make emergency calls to the fire department, rescue teams and local police department.

– Immediately notify postal security officers and appropriate area or district officials.

– Cordon off the scene and allow only those providing medical services to enter or remove any material unless authorized by a postal investigator.

– Account for all personnel. In addition to ensuring safety, emergency responders will want to interview some personnel.

– Closely coordinate instructions with the relevant local authorities.

– Notify the local utility companies of the incident and request technicians in case the gas or power supply need to be turned off.

21 Final considerations – contingency planning and incident response

21.1 Important considerations

– Bear in mind that severe damage could be inflicted to parts of the infrastructure, the post office or other parties involved, and public life.

– It is essential that normal business operations resume as quickly as possible.

– Minimize the impact as far as possible.

– Planning in advance for various scenarios will facilitate a more efficient recovery.

– Immediately safeguard damaged objects and facilities, e.g. against theft or looting.

– Immediately recover any capital goods, important documents, data and equipment.

– Keep site plans, etc., at an external location.

– Depending on the level of destruction and costs to repair, it may be necessary to vacate the building.

21.2 Steps in contingency planning

i Define the critical functions of business transactions – which key functions must be restored as quickly as possible in order to ensure continued operation? These key functions should be prioritized.

ii Target definition – what minimum standards of business transactions should be restored in which time periods? This must be determined for each operational area.

iii The resources needed to achieve the target must be described in terms of premises, staff, finances, channels of supply, industrial premises, logistics, communication, etc.

21.3 Staff

In order to keep staff motivated and working efficiently during a critical incident:

– Establish contact with staff immediately after the event and request they be on stand-by until specific instructions are issued.

– Provide clear information about when, where and for what operations staff will be required again.

– Provide transport where necessary.

– Make sure that staff are supplied with necessities when they resume work.

– Ensure the continued psychological support of those concerned.

21.4 Operating facilities

– If possible, move to other operating facilities temporarily.

– If necessary, temporarily outsource business areas and/or rent temporary premises nearby.

21.5 Data, documents and insurance policies

– Data should be backed up regularly.

– Essential data and duplicates of documents (e.g. phone lists) should be stored at another location if feasible.

– Insurance policies covering emergencies should be checked regularly and updated as needed.

– All confidential documents should be properly secured.

21.6 Summary

– Always take threats seriously.

– Procedures for responding to bomb threats and suspected explosive devices must be carefully prepared.

– Establishing clear procedures helps outside agencies respond effectively.

– Always alert the police.

– Time, distance and shielding are key to safety. Limit your time in an area suspected of containing an explosive device. Provide enough distance between you and the area to ensure you would not be injured if the device detonates. Take cover behind something large enough to protect you in the event the device detonates.

– Documentation is a fixed component of the continual improvement process → always have a contingency plan.

Appendix A

Organizations that can help with threat assessments

A threat can occur at multiple places in the mail delivery process. Different organizations can help at each point along the way.

1 At a postal facility (town/city)

2 In transit (road) within the country

3 In transit (road) outside the country

4 At the airport

5 In the air

In most instances, managers will be the first to assess the threat, followed by the postal security officer. Together, they will work with the local police, airline and airport authorities, and other specialized agencies as required. If the threat occurs in another country, this may require coordination with agencies located in the country of origin and/or delivery.

Postal operators should ensure that their security officers have a current list of telephone numbers for all relevant security officers and operational control centres, namely, within:

– the postal operator, i.e. postal security;

– other postal operators with which they exchange mail;

– carriers;

– airlines;

– airports;

– police;

– government security organizations (responsible for terrorism);

– other units that can assist with threat assessment.

Appendix B

Positive target identification

Some countries apply positive target identification (PTI) as a method of threat assessment.

The PTI method uses a form with various questions and boxes. The purpose is to eliminate hoax calls and ensure that credible threats are responded to appropriately.

Questions may cover the following:

– Has a specific building/site been identified? (Sub-questions would be: office, factory, sorting installation or airport premises?)

– Has a specific aircraft been identified? (Sub-questions would be: aircraft, flight number, route, destination airport, location or a vehicle en route to the airport?)

– Positive target identification:
  - Aircraft registration identified?
  - Location of explosive device identified?
  - Detailed description of device?
  - Specific description of item or place/means of concealment?
  - Reference to names of staff?
  - Terrorist group or other organization named?
  - Code word used?
  - Extortion or political demand made?
  - Specialized terminology used?
  - Other information offered indicating special knowledge?

– Background information:
  - Recent history of warnings and incidents;
  - Influence of current events;
  - Additional security measures in place;
  - Nature of call;
  - Assessment by police/others on the call (if applicable).

The answers to the above questions will help you gather sufficient information to make a decision:

– Doubts over security measures in force = **Red**;

– Confidence in security measures applied but extra security required in places = **Amber**;

– No target identified/confidence in security measures applied = **Green**.

Appendix C

List of contacts

Contact	*Telephone*	*Fax*
Postal security officer Name:	Office:	Office:
	Home:	Home:
E-mail:	Mobile:	
	Pager:	
Other (postal) security officer Name:	Office:	Office:
	Home:	Home:
E-mail:	Mobile:	
	Pager:	
Evacuation manager Name:		
Evacuation manager Name:		
Evacuation manager Name:		
Police		
Bomb disposal expert		
Fire		
Airport duty manager		
Airport security duty manager		
Airline duty manager		
Post office premises (……)		
Post office premises (……)		
Post office premises (……)		
Telephone switchboard		

Appendix D

Security procedures for suspicious items

When dealing with a suspicious item in the mail, remember that if it contains an explosive device, it has likely been designed to activate when it is opened or the contents removed (victim-activated). The following precautions should be taken when handling a suspicious mail item:

Do not:

– try to open the package or envelope;
– pass the item to another person for a double check;
– bend the item;
– tear the item or move it excessively;
– place the item near a heating appliance;
– place the item in water or in a humid room;
– cover the item;
– keep the item with other mail items.

Do:

– evacuate the area;
– alert your manager;
– alert the postal security officer;
– follow instructions;
– follow the contingency plan for your facility.

Appendix E

Profiling list

All items of mail, large and small, should be inspected (profiled) during the normal sorting process by postal staff. Staff should be trained to look for the following:

1 Addresses and restrictive markings

Markings that restrict the group of recipients, such as “confidential” or “personal”. Addresses that are typed, poorly handwritten, incomplete (no name), made out to the head of a department, cut and pasted or composed of a montage of individual letters. Items sent to high-profile or high-risk companies/persons, members of the government or public figures.

2 Return address

A generic or fictitious return address or no return address.

3 Type of packaging

Excessive wrapping, heavily taped or glued seams.

4 Excessive postage

Incorrect or excessive postage. More stamps than necessary for weight/destination to avoid weighing of the item at a post office counter.

5 Heavy/uneven weight distribution

Unbalanced, could contain loose articles, powder or liquids.

6 Stiffness

To prevent the IID/IED from breaking apart in transit, the maker may add stiff material. (Do not bend suspicious packages.)

7 Protruding wires or foil or pin holes in the wrapping

Used to arm or activate the device.

8 Grease marks

Some explosives leave a residual greasy stain on the packaging paper.

9 Other suspicious signs

Staff should be made aware of any current threat information that may help with the identification of IEDs or IIDs in the mail.

Appendix F

Example of a telephone bomb threat report

Company: _____

Department: _____

Name: _____

Date: _____ Time of call: _____

Message (exact words):

Where is the bomb?

When will it explode?

What does the bomb look like?

Why you are doing this?

Who are you? What organization do you represent?

Where are you now?

Try to assess the following:

– Age and sex of the caller.
– Was the caller irrational, rambling or possibly intoxicated?
– Did the caller have a distinctive accent?
– Did it sound as if the caller was reading from a prepared statement?
– Was the call made from a private line, call box or mobile phone?
– Was there any significant background noise?

Keep the caller on the line as long as possible. This will give you time to trace the call and gather background information that can assist the security officer in making a threat assessment.

Finally, remember to keep the original telephone message regarding the bomb threat – it may be required as evidence in a court of law.