PAS 97:2021

Mail screening and security – Specification

CPNI
Centre for the Protection of National Infrastructure

bsi.

Publishing and copyright information

Published by BSI Standards Limited 2021.

ISBN 978 0 539 04174 3

ICS 13.310

Publication history

First published March 2009
Second edition January 2012
Third edition October 2015
Fourth (present) edition March 2021

Contents

Foreword

This Publicly Available Specification (PAS) was sponsored by the Centre for the Protection of National Infrastructure (CPNI). Its development was facilitated by BSI Standards Limited and it was published under licence from The British Standards Institution (BSI). It came into effect on 31 March 2021.

Acknowledgement is given to the following organizations that were involved in the development of this PAS as members of the steering group:

- Bank of America
- BBC
- British Transport Police
- Canary Wharf Management
- Counter Terrorism Policing South East
- Centre for the Protection of National Infrastructure
- Credit Suisse UK
- Deutsche Bank
- Eastern Region Special Operations Unit – Counter Terrorism Policing
- PosteRoute Ltd
- Royal Mail Group
- Swiss Post Solutions
- Scottish Parliament
- Vodafone Ltd
- West Midlands Police

Acknowledgement is also given to the members of a wider review panel who were consulted in the development of this PAS.

This PAS is not to be regarded as a British Standard. It will be withdrawn upon publication of its content in, or as, a British Standard.

The PAS process enables a specification to be rapidly developed in order to fulfil an immediate need in industry. A PAS can be considered for further development as a British Standard, or constitute part of the UK input into the development of a European or International Standard.

Supersession

This PAS supersedes PAS 97:2015, which is withdrawn.

Use of this document

It has been assumed in the preparation of this PAS that the execution of its provisions will be entrusted to appropriately qualified and experienced people, for whose use it has been produced.

Presentational conventions

In this PAS, the word "shall" indicates requirements. The word "should" is used to express recommendations of this standard. The word "may" is used in the text to express permissibility, e.g. as an alternative to the primary recommendation of the clause. The word "can" is used to express possibility, e.g. a consequence of an action or an event. All wording without use of these verbs is general commentary that provides a framework for useful understanding of the provisions of this standard. Paragraphs marked "NOTE" offer particular guidance in understanding or clarifying the associated requirement.

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a PAS cannot confer immunity from legal obligations.

Introduction

Even in this electronic age, most businesses and other organizations rely on the ability to receive and send physical items of mail. As an essential part of normal operations, mail presents various potentially significant vulnerabilities. Mail streams into and within an organization provide a vector for malicious attacks and scope for other security incidents, all of which can endanger life and adversely affect the day-to-day business of the organization, as well as its reputation.

Attacks might be intended to cause physical damage to property, harm to individuals, to create fear or merely to cause disruption. Conversely, it is also quite possible for perfectly benign objects to appear suspicious, causing disruption through emergency responses that prove unnecessary. In addition, incoming and outgoing mail streams might contain valuable items or sensitive information that warrant protecting from loss or theft.

Mail screening and security measures can be used to reduce the risk and impact of such incidents. This PAS aims to assist organizations in identifying and implementing appropriate postal security measures that meet their particular needs.

Too few or inappropriate measures increase the risk of significant security incidents that harm the organization and its business. Excessive measures are likely to be an unnecessary expense and might otherwise reduce the efficiency of the organization, for example by causing delays or using scarce staff and space resources.

In working to identify and implement the appropriate measures for an organization, it is important to consider factors both within and external to the organization as well as potential future changes to these. For example, the nature of the organization's business could change in a way that affects mail throughput requirements, as could the public profile of the organization in a way that makes it more likely to be targeted by single-issue groups, terrorists or disaffected individuals.

While not exhaustive, the following case studies highlight different threats and how they were addressed.

Case Study A – US anthrax letters, Autumn 2001

In September and October 2001, letters containing *Bacillus anthracis* spores were mailed to several news media offices and two US Democrat Senators. Five people died of inhalational anthrax and more than a dozen others became seriously ill. Thousands of employees of the US Postal Service and government offices that could have been exposed were given antibiotics as a precaution. Dozens of buildings were contaminated as a result of the mailings. The attack had a severe impact on mail services across the United States as many postal facilities had to close for decontamination. One building took three years to reopen after decontamination at a cost of many tens of millions of dollars.

US Federal prosecutors eventually declared a scientist employed in the government's bio-defence laboratories as the sole perpetrator, though his motives for the attacks were unclear.

Case Study B – UK letter bomb campaign, 2007

In January and February 2007, there was a targeted mail campaign in the UK against seven companies and government agencies which the perpetrator believed were connected to a rise in a "surveillance society". Relatively unsophisticated explosive devices were used, most of which functioned on opening causing minor injuries to the hands and upper bodies of the persons handling the items and other persons nearby. Due to the different ways in which organizations handle incoming mail, those who opened the letters and were injured were not necessarily the intended targets for the devices. In two cases the items were intercepted by trained and vigilant mail room operators and dealt with safely using practised escalation procedures, resulting in minimum disruption to the organizations concerned.

In September 2007, Miles Cooper, a school caretaker from Cambridge, was found guilty of a variety of charges in relation to the letter bomb campaign, and received an indeterminate prison sentence.

Case Study C – UK hoax campaign, 2012

A series of hoax "anthrax" letters were sent to high profile government officials, including the Deputy Prime Minister, in the summer and autumn of 2012. The letters were intercepted at a mail screening centre, and the substance found to be non-hazardous. If the letters had not been intercepted the campaign would undoubtedly have caused concern and disruption.

Ruth Augustus was found guilty of six counts of hoaxes involving noxious substances and was sentenced to a two-year community order in addition to receiving mental health treatment.

Case Study D – US ricin letters, 2013

On 16 April 2013, an envelope addressed to a US Senator was intercepted at the US Capitol's offsite mail facility in Washington DC and tested positive for ricin. The following day a second envelope, this time addressed to the President of the United States, was intercepted and again tested positive for ricin. A further letter containing ricin reached its intended recipient, however the individual was not harmed.

Everett Dutschke was charged in June 2013 for developing and possessing ricin toxin and subsequently mailing ricin-laced, threatening letters, including one that threatened bodily harm to the President of the United States. He was sentenced to 25 years in prison.

The events sparked numerous copycat incidents with individuals mailing ricin to a senior judge and the Mayor of New York.

Case Study E – UK parcel bombs, 2014

In February 2014 a series of parcel bombs were sent to several British Armed Forces Careers Offices across England. All the devices were contained within envelopes which were addressed by hand. A group linked to Northern Irish terrorism claimed responsibility for the packages in a statement made to the *Irish News*. If they had not been discovered, the crude but potentially viable devices were likely to have caused harm to their victims.

Case Study F – UK series of white powder incidents, 2016

Over the period of one day in July 2016, five incidents were reported of white powder being delivered to Muslim centres, mosques, a government building and a mail screening service in London. One envelope was said to feel suspicious and lumpy, with powder and offensive messages subsequently found inside. The organization called the police and specialist officers attended, and the powder was discovered not to be hazardous. One building was evacuated for more than two hours on discovery of the package which was opened to reveal white powder. This highlights the importance of early recognition of potential suspicious indicators in mail, before (and in the event of) being delivered to the recipient, as well as the need for a robust response procedure that must be in place to minimize further impact.

Case Study G – UK white powder incident, 2018

In February 2018, a security incident was triggered when a small package containing white powder was delivered to a UK government department's office. Specialist officers examined the package at the scene, which was later found to be non-harmful. The office affected was isolated while the rest of the building remained open as usual. Security alerts were also minimized to avoid further alarm. The proportionate response procedures that were put into action ensured business continuity ensued while the incident was being addressed.

Case Study H – UK postal devices, 2019

In March 2019, a number of improvised devices were sent to transport hubs and other locations in England and Scotland. The devices were contained within padded envelopes inside plastic postal bags. One of the devices was opened and caught fire, though thankfully no one was injured.

At a number of the other sites, staff handling the mail deemed the items suspicious and implemented response procedures, evacuating the surrounding area and calling the police. Specialist officers then attended and made the devices safe.

The quick and effective response of mail handling staff, and timely information sharing between the organizations involved, meant that although there was disruption to some areas of the sites, their main business was unaffected. If they had not been discovered, these devices could have caused harm to their recipients.

Case Study I – Internal mail screening for non-malicious threats

Whilst security is an important issue for the oil and gas industry, safety is paramount; hence alcohol and drugs are prohibited on all offshore oil and gas installations. Employees and contractors are required to declare all medical conditions and any drugs prescribed to them to treat these conditions. Mail to offshore installations is routed internally within the respective organization – it is received at a company office on land where it is screened for alcohol and drugs (both prescribed and illegal), as well as hazardous materials and items, before being transferred offshore.

1 Scope

This PAS specifies requirements and gives recommendations for mail screening, set in the broader context of postal security. It is intended for use by those responsible for planning, delivering or procuring mail handling and screening services within organizations, as well as commercial providers of such services.

It specifies measures to assist businesses and other organizations in identifying and minimizing the impact of items of mail that represent a threat, or could otherwise cause concern or disruption. It also addresses broader postal security measures aimed at ensuring all incoming, outgoing and internal mail streams are managed so as to minimize the risk of loss or theft of valuable or sensitive items or information.

This PAS concentrates on letters and small parcels entering the organization from any external source, including public/commercial postal services, by hand or by courier delivery.

Whilst many of the principles detailed in this PAS can also be applied to improving the security of other, larger-scale deliveries, these are not explicitly covered.

The security of electronic mail and associated IT systems is outside the scope of this PAS.

This PAS does not propose a single standard of postal security and screening. Instead, it sets out to assist organizations in assessing their particular level(s) of risk and selecting and implementing commensurate security measures whether onsite or offsite, delivered in-house or outsourced. A series of screening levels (1 to 5) is defined in terms of progressively more complex screening measures; this is complemented by a series of physical protection classes (A to D) that describe incremental physical protective measures for mail rooms and personnel.

NOTE *Another factor contributing to the overall level of protection an organization derives from its postal security measures is the location of its mail facilities.*

2 Terms and definitions

For the purposes of this PAS, the following terms and definitions apply.

2.1 deliveries

goods received by an organization

NOTE *This includes mail and a broad range of other, often larger, items (for example cleaning, catering and office supplies and equipment) which present different challenges.*

2.2 mail

letters and small packages, which could be delivered by a commercial postal operator or courier company, be hand delivered or originate within the organization

NOTE *Whilst "post" and "mail" are commonly used interchangeably, the term "mail" is used throughout this PAS (with "postal" used as the corresponding adjective).*

2.3 mail handling

all aspects of moving mail (**2.2**) around within an organization, including collection, sorting, distribution and delivery

2.4 mail room

room or multi-room facility where mail (**2.2**) is sorted and/or screened

2.5 mail screening

use of manual or automated methods to identify hazards and other causes of disruption associated with items of mail (**2.2**)