Software Engineering Institute

CERT Resilience Management Model—Mail-Specific Process Areas: International Mail Transportation (Version 1.0)

Julia H. Allen
Gregory Crabb (United States Postal Inspection Service)
Pamela D. Curtis
Sam Lin (United States Postal Inspection Service)
Nader Mehravari
Dawn Wilkes (United States Postal Inspection Service)

August 2014

TECHNICAL NOTE
CMU/SEI-2014-TN-012

CERT Division

http://www.sei.cmu.edu

Carnegie Mellon

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
AUG 2014		

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
CERT Resilience Management Model - Mail-Specific Process Areas: International Mail Transportation (Version 1.0)	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University ,Software Engineering Institute,Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Developing and implementing measurable methodologies for improving the security and resilience of a national postal sector directly contribute to protecting public and postal personnel, assets, and revenues. Such methodologies also contribute to the security and resilience of the mode of transport used to carry mail and the protection of the global mail supply chain. Since 2011, the U.S. Postal Inspection Service (USPIS) has collaborated with the CERT? Division at Carnegie Mellon University?s Software Engineering Institute to improve the resilience of selected U.S. Postal Service (USPS) products and services. The CERT Resilience Management Model (CERT-RMM) and its companion diagnostic methods served as the foundational tool for this collaboration. This report includes one result of the USPIS/CERT collaboration. It is an extension of CERT-RMM to include a new mail-specific process area for the transportation of international mail. The purpose is to ensure that all international mail is transported in accordance with the standards established by the Universal Postal Union (UPU), which is the governing body that regulates the transportation of international mail.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**53**	

This material is based upon work funded and supported by United States Postal Service under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of United States Postal Service or the United States Department of Defense.

This report was prepared for the
SEI Administrative Agent
AFLCMC/PZM
20 Schilling Circle, Bldg. 1305, 3rd floor
Hanscom AFB, MA 01731-2125

DM-0001502

Table of Contents

List of Figures

List of Tables

Abstract

Developing and implementing measurable methodologies for improving the security and resilience of a national postal sector directly contribute to protecting public and postal personnel, assets, and revenues. Such methodologies also contribute to the security and resilience of the mode of transport used to carry mail and the protection of the global mail supply chain. Since 2011, the U.S. Postal Inspection Service (USPIS) has collaborated with the CERT® Division at Carnegie Mellon University's Software Engineering Institute (SEI) to improve the resilience of selected U.S. Postal Service (USPS) products and services. The CERT Resilience Management Model (CERT-RMM) and its companion diagnostic methods served as the foundational tool for this collaboration.

This report includes one result of the USPIS/CERT collaboration. It is an extension of CERT-RMM to include a new mail-specific process area for the transportation of international mail. The purpose is to ensure that all international mail is transported in accordance with the standards established by the Universal Postal Union (UPU), which is the governing body that regulates the transportation of international mail.

Introduction

In December 2011, the U.S. Postal Inspection Service (USPIS) asked CERT staff to develop new mail-specific process areas (PAs) to manage the resilience of mail throughout its lifecycle—from induction to delivery. The initial scope of this effort included mail acceptance, revenue confirmation, mail security, mail transport, and mail custody.

The CERT® Resilience Management Model (CERT-RMM) [Caralli 2011], which was developed by the CERT Division at Carnegie Mellon University's Software Engineering Institute (SEI), and its companion diagnostic methods served as the foundational tool for this collaboration. CERT-RMM is a capability-focused maturity model for improving an organization's management of operational resilience activities across the domains of security management, business continuity management, and aspects of information technology operations management. These improvements enable high-value services to meet their missions consistently and with high quality, particularly during times of stress and disruption.

The USPIS objectives for this project included the following [Crabb 2012, Joch 2013]:

- Define common criteria for assuring that U.S. Postal Service (USPS) products are resilient.
- Evaluate business partners and customer operations in their handling of mail.
- Use these new PAs in conjunction with other selected CERT-RMM PAs to evaluate new and existing USPS products, services, suppliers, and partners, in terms of their security and resilience.
- Assure that each product's contribution to USPS revenue is commensurate with services delivered.
- Identify revenue collection gaps more quickly.

The development project commenced in January 2012 and was an active collaboration between USPIS subject matter experts and CERT staff. The architecture of the mail-specific PAs follows that of the existing 26 PAs described in CERT-RMM. The scope and content of these PAs evolved significantly during the course of the development project. In July 2012, initial outlines for four mail-specific PAs—Mail Induction (MI), Mail Revenue Assurance (MRA), Mail Transportation (MT), and Mail Delivery (MD)—were accepted by the USPIS, as well as an initial draft of the MRA PA.

The PAs specific to the induction of mail and to mail revenue assurance were pilot tested extensively during the Express Mail projects described in an SEI technical note titled *Improving the Security and Resilience of U.S. Postal Service Mail Products and Services Using the CERT® Resilience Management Model* [Crabb 2014]. In April 2013, outlines for all four mail-specific PAs were accepted as baselined by the USPIS, and in July 2013, baselined

® CERT is a registered mark of Carnegie Mellon University.

versions of two complete PAs, MI and MRA, were accepted by the USPIS [Allen 2014a, Allen 2014b].

Following this initial effort, the USPIS asked CERT to extend the goals and practices contained within the MT outline for U.S. domestic mail to address international mail transportation as defined by the UPU. The UPU, headquartered in Berne, Switzerland, is a unit of the United Nations that regulates the postal services of 192 member countries. These postal services form the largest physical distribution network in the world.

The Postal Security Group (PSG) of the UPU develops global and regional security strategies to assist postal operators in their common security missions. PSG members are security experts from a number of UPU member countries. For the past 17 years, the Chief Postal Inspector of the USPIS has chaired the PSG, which includes ensuring the resilience and security of international mail during its transportation.

The International Mail Transportation Process Area is presented in this report.

International Mail Transportation

Purpose

The purpose of the CERT-RMM International Mail Transportation (IMT) process area is to ensure that all international mail is transported in accordance with UPU standards.

NOTE: The scope of this version is air transport. The scope will be expanded to include surface transport in the next phase of development.

Outline

IMT:SG1 Establish Standards for International Mail Transportation

Standards for international mail transportation are established and maintained.

IMT:SG1.SP1 Establish Standards for International Mail Transportation

Standards for the transportation of international mail are identified, established, and maintained.

IMT:SG2 Transport International Mail

International mail is processed for transportation and transported in accordance with standards.

IMT:SG2.SP1 Process Outbound International Mail

Outbound international mail is processed for transportation in accordance with standards.

IMT:SG2.SP2 Transport Outbound International Mail

Outbound international mail is transported to destination processing facilities in accordance with standards.

IMT:SG2.SP3 Transport Inbound International Mail

Inbound international mail is transported to destination processing facilities in accordance with standards.

IMT:SG2.SP4 Process Inbound International Mail

Inbound international mail is processed in accordance with standards.

IMT:SG3 Manage Risks to International Mail During Transportation

Operational risks to international mail during transportation are identified and addressed.

IMT:SG3.SP1 Identify and Assess Risks to International Mail During Transportation

Operational risks to international mail during transportation are periodically identified and assessed.

IMT:SG3.SP2 Address Risks to International Mail During Transportation

Identified operational risks to international mail during transportation are addressed.

IMT:SG4 Control International Mail During Transportation

Controls to protect international mail during transportation are established and maintained in accordance with standards.

IMT:SG4.SP1 Control Access to International Mail During Transportation

Controls are established and maintained to assure access to international mail during transportation in accordance with standards.

IMT:SG4.SP2 Control Availability of International Mail During Transportation

Controls are established and maintained to assure availability of international mail during transportation in accordance with standards.

IMT:SG4.SP3 Control Sanctity of International Mail During Transportation

Controls are established and maintained to assure sanctity of international mail during transportation in accordance with standards.

IMT:SG4.SP4 Control Custody of International Mail During Transportation

Controls are established and maintained to assure custody of international mail during transportation in accordance with standards.

IMT:SG4.SP5 Control Visibility of International Mail During Transportation

Controls are established and maintained to assure visibility of international mail during transportation in accordance with standards.

IMT:SG5 Manage International Mail Discrepancies During Transportation

Discrepancies during the transportation of international mail are identified and addressed.

IMT:SG5.SP1 Establish and Maintain International Mail Discrepancy Plans for Transportation

Plans and procedures for managing discrepancies during the transportation of international mail are established and maintained.

IMT:SG5.SP2 Identify and Address International Mail Discrepancies During Transportation

Discrepancies during the transportation of international mail are identified and addressed in accordance with plans and procedures.

Introductory Notes

A resilient international mail transportation service is critical to the global postal and shipping sector. In addition, every sector of the economy depends on the service providers in the postal and shipping sector to deliver time-sensitive letters, packages, and other shipments. In particular, the banking and finance, commercial facilities, government facilities, and healthcare and public health sectors rely heavily on the postal and shipping sector for the shipment and delivery of critical documents and packages.

Mail is an important asset for connecting the world's population, businesses, and governments. Through universal service mandates, many countries establish requirements

for postal administrations (Posts) to provide mail services to all citizens. Posts manage a complex set of relationships to accept, process, transport, and deliver mail. The support of this supply chain is necessary for Posts and their service providers to manage their mail services in an operationally resilient manner.

Mail is subject to a number of threats that may prevent the successful completion of its transportation from one country's International Mail Processing Center (IMPC) to another country's IMPC. These threats may include natural and man-made disasters, damage, theft, fraud, and terrorism. Natural disasters such as hurricanes, earthquakes, and fires can destroy or inhibit the timely transportation of mail. Employees, service providers, and the public can steal mail. On occasion, mail has been used to distribute bombs, toxic chemicals, biological agents, and radioactive material. In addition, the many systems that are used to scan, sort, screen, and process mail are subject to inadvertent and malicious compromise, which can result in damage, delay, and loss of mail. The protection of the mail is the subject of national and international laws that define criminal acts and punishments involving the misappropriation of mail.

Mail is defined as the combination of the category (UPU code list 115), class (UPU code list 116), and subclass (UPU code list 117) of items that are accepted, transported, and delivered by Posts. Category includes airmail or priority mail, SAL (surface air lift) mail, and surface mail. Class includes letters, parcels, EMS (Express Mail Service), and empty receptacles. Supplementary services are also available, including registration service, insurance, recorded delivery, and cash on delivery.

Effectively managing the resilience of mail during transportation is critical to support the goals of the UPU, the UPU Postal Security Group, and its member postal administrations. Operational resilience is an organization's ability to protect its critical assets and keep essential services and processes operating, particularly during times of stress and disruption. For mail transportation, resilience is the ability of IMPCs,[1] postal administrations, and the international postal network to protect mail and protect and sustain all of the services and processes that handle mail from mail acceptance to mail delivery, particularly during times of disruption and stress.

UPU goals relevant to resilience include [1]

- prevention of injuries to people due to the carriage of dangerous goods in the mail
- prevention of loss or theft of mail entrusted to Posts
- prevention of revenue and asset losses by Posts
- preservation of customer confidence in the Posts

Meeting these goals requires the identification and establishment of UPU standards that pertain to mail resilience and implementing controls to ensure that these standards are

[1] An IMPC can be an Office of Exchange (OE), a mail unit, or both, as shown in Figures 1 and 3. An OE creates or receives despatches. A mail unit creates or receives consignments. In this PA, IMPC is the most commonly used term to encompass both roles [2].

satisfied throughout the mail transportation lifecycle. The UPU has a robust set of standards to properly manage the lifecycle of mail when it comes into the custody of a specific national Post and leaves that custody (including when mail becomes the custodial responsibility of airline carriers and other transportation service providers), as shown in Figure 1.

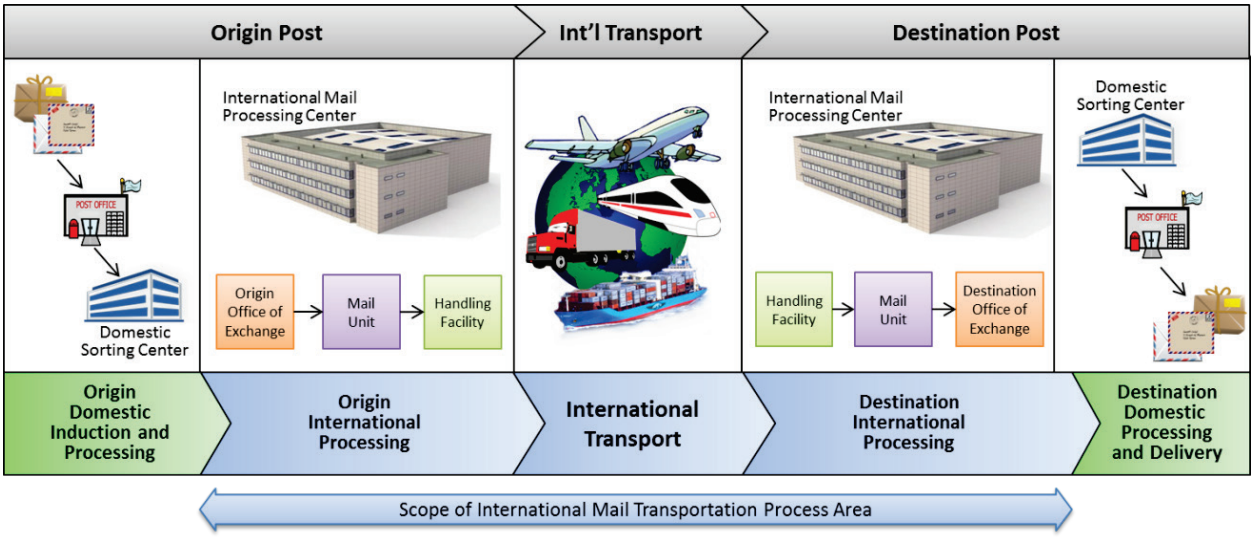

Figure 1: International Mail Lifecycle

History shows that as standards improve, the quality of the product that is subject to those standards improves. There are many UPU and national standards that are applicable to the transportation of international mail. Each IMPC and postal administration determines which standards are required for their operations. A few of these standards are described in IMT:SG1, Establish Standards for International Mail Transportation, and are identified as examples in subsequent specific goals and practices. Posts need to ensure that they satisfy the many performance standards, compliance obligations, and customer expectations for the transportation of mail.

In addition to UPU standards and goals, resilience requirements should form the basis for actions taken to protect mail during transportation. Resilience requirements for postal items include

- access: the authorized ability, right, or privilege of a person or system to sort, scan, screen, view, or take physical possession of a postal item.
- availability: the quality of postal items being accessible in a timely fashion. Mail must not be lost, stolen, or unnecessarily delayed.
- sanctity: the quality of postal items being preserved from damage, alteration, and unlawful disclosure. Mail must be kept in the condition intended for the sender and suitable for being transported.
- custody: the state of postal items being in the immediate charge and control of authorized personnel from induction through delivery

- visibility: the ability to track postal items from induction to delivery by means such as electronic mailing documentation, barcodes on postal items and containers, and in-process scanning while mail is in the postal network

These resilience requirements are established based on the mail category, class, subclass, and supplementary services and in accordance with applicable UPU standards and national and international laws. The appropriate type and level of protective controls should be designed, implemented, and monitored to meet these requirements.

This CERT Resilience Management Model (CERT-RMM) supplemental, mail-specific process area describes key goals and practices that can be used as a standalone evaluation tool or in conjunction with other CERT-RMM process areas to evaluate the resilience of international mail during transportation and as required by UPU standards. Organizations to be evaluated may include national Posts, transportation mail service providers, and other postal handling organizations authorized by Posts, such as air carriers.

All references to "mail" and "postal items" in this process area refer to international mail unless specifically described as national or domestic mail.

Scope

The scope of this process area is as shown in the bar across the bottom on Figure 1. Outbound international mail is received at a country's IMPC. It is scanned, sorted, screened, and processed, including any postal items that require inspection by Customs and national export control systems and personnel. Before mail leaves the IMPC, it is assigned to receptacles, receptacles are assigned to despatches, and receptacles are assigned to consignments. Each consignment is assigned to a specific air carrier flight. Once mail departs the IMPC and arrives at a designated air carrier facility or warehouse, it is considered to be in the custody of that air carrier. Consignments are processed, transported to and loaded onto their designated aircraft, and delivered to the destination country. While enroute, mail may be subjected to transshipment or transit processing in an intermediate country. This completes the outbound mail portion of the transportation lifecycle.

From a destination country's IMPC perspective, inbound international mail is processed in the reverse. Mail is received at the origin country's air carrier facility from the origin IMPC and is in the custody of the air carrier. Consignments are processed, transported to and loaded onto their designated aircraft, and delivered to the destination country. While enroute, mail may be subjected to transshipment or transit processing in an intermediate country. At the destination airport, mail is unloaded from the aircraft, transported to the destination IMPC, and scanned by the air carrier. Mail is now considered to be in the custody of the national Post responsible for that IMPC. Mail is removed from receptacles, scanned, sorted, screened, and processed, including any postal items that require inspection by Customs systems and personnel and national postal inspectors. Once international mail completes Customs inspection, it is considered out of scope for this process area.

Related Process Areas

The identification of mail revenue standards and the assurance of mail revenue (postage affixed, payment, discrepancies, and fraud) are addressed in the CERT-RMM Mail Revenue Assurance process area.

Requirements for the receipt of payment are described in the CERT-RMM Mail Revenue Assurance process area.

The protection of mail during induction is addressed in the CERT-RMM Mail Induction process area.

Compliance with mail transportation standards is addressed in the CERT-RMM Compliance process area.

The management of the internal control system that ensures the resilience of mail and mail services during transportation is addressed in the CERT-RMM Controls Management process area.

The assignment of resilience requirements to the physical IMPC facilities where mail transportation activities are conducted and other physical, environmental, and geographical controls to support the resilience of mail and mail services during transportation are managed in the CERT-RMM Environmental Control process area.

The establishment and management of controls relating to the integrity and availability of technology assets used for mail and mail services during transportation are defined in the CERT-RMM Technology Management process area.

The processes to identify and analyze events, detect incidents, and determine an appropriate organizational response for events affecting mail and mail services during transportation are addressed in the CERT-RMM Incident Management and Control process area.

The controls to ensure the continuity of essential operations of mail services if a disruption occurs during transportation as a result of an incident, disaster, or other disruptive event are addressed in the CERT-RMM Service Continuity process area.

Ensuring that resilience requirements for mail are met by service providers and other external entities involved during transportation is addressed in the CERT-RMM External Dependencies Management process area.

Controls to manage the performance of people in support of the resilient management of mail during transportation are addressed in the CERT-RMM Human Resource Management process area.

Inventories and gap analysis of skills required for the resilient management of mail during transportation are addressed in the CERT-RMM Human Resource Management process area.

The provision of awareness and training to staff necessary for the resilient management of mail during transportation is addressed in the CERT-RMM Organizational Training and Awareness process area.

Summary of Specific Goals and Practices

IMT:SG1 Establish Standards for International Mail Transportation
- IMT:SG1.SP1 Establish Standards for International Mail Transportation

IMT:SG2 Transport International Mail
- IMT:SG2.SP1 Process Outbound International Mail
- IMT:SG2.SP2 Transport Outbound International Mail
- IMT:SG2.SP3 Transport Inbound International Mail
- IMT:SG2.SP4 Process Inbound International Mail

IMT:SG3 Manage Risks to International Mail During Transportation
- IMT:SG3.SP1 Identify and Assess Risks to International Mail During Transportation
- IMT:SG3.SP2 Address Risks to International Mail During Transportation

IMT:SG4 Control International Mail During Transportation
- IMT:SG4.SP1 Control Access to International Mail During Transportation
- IMT:SG4.SP2 Control Availability of International Mail During Transportation
- IMT:SG4.SP3 Control Sanctity of International Mail During Transportation
- IMT:SG4.SP4 Control Custody of International Mail During Transportation
- IMT:SG4.SP5 Control Visibility of International Mail During Transportation

IMT:SG5 Manage International Mail Discrepancies During Transportation
- IMT:SG5.SP1 Establish and Maintain International Mail Discrepancy Plans for Transportation
- IMT:SG5.SP2 Identify and Address International Mail Discrepancies During Transportation

Specific Practices by Goal

IMT:SG1 Establish Standards for International Mail Transportation

Standards for international mail transportation are established and maintained.

The purpose of establishing regulations, standards, policies, operating procedures, and other specifications (standards for short) for the transportation of mail is to ensure that international postal administrations (including contractors, vendors, and other service providers) understand their responsibilities for origin processing, transportation, and destination processing of mail and for entering mail into national mailstreams. Such standards provide the foundation for ensuring the resilience of mail during transportation and helping postal administrations manage the transportation of mail between countries.

To ensure that postal items are adequately protected during transportation, standards specify resilience requirements that are assigned to postal items based on their category, class, and subclass. Thus standards for access to mail and for the availability, sanctity, custody, and visibility of mail must be established and maintained.

The specification of resilience requirements in mail transportation standards support the design, implementation, and monitoring of controls to ensure resilience requirements for all postal items are met (refer to IMT:SG4, Control International Mail During Transportation).

IMT:SG1.SP1 Establish Standards for International Mail Transportation

Standards for the transportation of international mail are identified, established, and maintained.

According to the *Catalogue of UPU Standards* [3],

> *Standards are important prerequisites for effective postal operations and for interconnecting the global network. The UPU's Standards Board develops and maintains a growing number of standards to improve the exchange of postal-related information between postal operators and promotes the compatibility of UPU and international postal initiatives. It works closely with postal handling organisations, customers, suppliers and other partners, including various international organisations. The Standards Board ensures that coherent standards are developed in areas such as electronic data interchange (EDI), mail encoding, postal forms and meters.*

UPU standards[2] specify what mail can be transported and in what manner it can be transported—and therefore what postal administrations can accept for origin processing, transportation, and destination processing.

Such standards define what postal items are eligible to be transported via international air carriers because they meet criteria specified by standards and are not prohibited.

The *UPU Letter Post Manual* [4] provides the articles and detailed regulations and rules to which member countries have agreed with respect to the handling of letters. The *UPU Parcel Post Manual* [5] provides the articles and detailed regulations and rules to which member countries have agreed with respect to the handling of parcels. With respect to postal security, these manuals state the following:

> *Member countries and their designated operators shall adopt and implement a proactive security strategy at all levels of postal operations to maintain and enhance the confidence of the general public in the postal services, in the interests of all officials involved. This strategy shall include the exchange of information on maintaining the safe and secure transport and transit of mails between member countries and their designated operators.*

The *UPU S58 Postal security standards – General security measures* defines the minimum physical and process security requirements applicable to critical facilities within the postal network [6]. The *UPU S59 Postal security standards – Office of exchange and international airmail security* defines minimum requirements for securing operations relating to the transport of international mail, including secure supply chain, secure environment, and screening [7]. S58 and S59 define mandatory measures to better screen and take custody of international mail and to apply the security standards to critical facilities, such as

[2] http://www.upu.int/en/activities/standards/standards-documents.html

international offices of mail exchanges, which process arriving and departing international mail.

The *UPU Standards Glossary* [8] defines many of the terms, acronyms, symbols, and abbreviations that are used in other UPU standards. UPU definitions have been used throughout this PA.

The *UPU Postal Transport Guide* [2] serves as an information source for Postal staff dealing with the transportation and transit of mail, in all of its modes (air, maritime, and surface).

The *UPU Transport Service Agreement template* [9] specifies the agreement between a Post that wishes to contract with an air transport company to ensure the air conveyance of postal items and a carrier that agrees to provide the conveyance of postal items to the Post under the terms and conditions specified in the agreement.

Standards specific to origin processing, transportation, and destination processing of postal items and standards for access to mail and for the access to and availability, sanctity, custody, and visibility of mail are designated in Table 1.

Table 1: Selected UPU Standards and Their Areas of Applicability

	Origin Processing	Transportation	Destination Processing	Access	Availability	Sanctity	Custody	Visibility
Letter Post Manual [4]				x	x	x	x	x
Parcel Post Manual [5]				x	x	x	x	x
S58 [6]				x	x	x		
S59 [7]				x	x	x	x	x
Standards Glossary [8]	x	x	x					
Postal Transport Guide [2]	x	x	x				x	x
Transport Service Agreement template [9]	x	x	x	x			x	

Compliance obligations that may result in or form the basis for mail transportation standards are identified and managed in the CERT-RMM Compliance process area.

Typical Work Products

1. Standards for origin processing of outbound postal items (including export control)
2. Standards for transportation of postal items, both outbound from a country and inbound to a country
3. Standards for destination processing of inbound postal items (including Customs)

4. Standards for access to postal items
5. Standards for availability of postal items
6. Standards for sanctity of postal items
7. Standards for custody of postal items
8. Standards for visibility of postal items
9. Procedures for communicating standards
10. Procedures for ensuring that postal administration personnel, mailers, and service providers adhere to standards

Subpractices

1. Identify the most current versions of all regulations, standards, policies, operating procedures, and supporting specifications and guidelines that affect mail transportation practices and resilience requirements for postal items during transportation.
2. Communicate mail transportation standards to all affected parties (postal administrations, mailers, service providers, etc.).
3. Ensure that postal administration personnel adhere to standards.
4. Ensure that mailers adhere to standards.
5. Ensure that service providers adhere to standards.

The *General Information on UPU Standards* defines the following subpractices, which, by reference, may be relevant to SG1 [10]:

- Develop and publish new standards as needed to reflect changes in mail transportation practices.
- Follow established procedures for revising existing standards.
- Document approved revisions to existing standards in all affected publications.
- Make standards available to mailers, postal administrations, and other users of the standards in appropriate locations and formats (most often accomplished via the UPU website).

IMT:SG2 Transport International Mail

International mail is processed for transportation and transported in accordance with standards.

Transport is defined as the conveyance of mail from one location (origin) to another location (destination) and, in the case of international mail, from one country to another country. The scope of this goal, as depicted in Figure 1, includes the following:

- the processing of outbound international mail at the origin IMPC
- the transportation of outbound international mail from the origin IMPC to the destination IMPC

- the transportation of inbound international mail from the origin IMPC to the destination IMPC
- the processing of inbound international mail at the destination IMPC

Applicable UPU standards may include the *Letter Post Manual* [4], the *Parcel Post Manual* [5], the *Postal Transport Guide* [2], the *Transport Service Agreement template* [9], S58 [6], and S59 [7]. (Refer to IMT:SG1.SP1 for additional guidance about standards.)

Outbound International Mail

Once outbound international mail is inducted (accepted) by national postal administrations and brought to the IMPC, it must be properly processed and then transported to its final destination. This process begins with postal items being separated by mail category, class, and subclass, as defined by UPU standards to include letters, parcels, and Express Mail Service (EMS). This is followed by mail sortation (destination country, IMPC, and postcode/delivery zone number [4]) and various forms of screening. Sortation also includes allocating mail to assigned receptacles, allocating receptacles to one or more despatches, and assigning receptacles to consignments. Once these activities are accomplished, outbound mail is assigned and routed to a specific air carrier for transportation to the destination IMPC.

Receptacles, Despatches, and Consignments

The UPU term “receptacle” is used to describe a physical entity that can be used to contain or carry mail so as to assist in its handling or transportation as a unit. A receptacle may include individual postal items, mailbags, trays, wheeled containers (roller cages), pallets and pallet-based containers, and airfreight containers (often referred to as cans or unit load devices [ULDs]). Oversized parcels that do not fit into receptacles (bags) are transported separately as outside pieces and given a unique receptacle-ID.

Each receptacle has a unique receptacle-ID. This ID (reflected as a barcode) is created by origin IMPCs and used by operators, carriers, and Posts to track the location of receptacles and connect receptacles to despatches. By scanning the receptacle-ID, the despatch-ID and the despatch-series are automatically captured. Thus a single scan captures the origin and destination IMPCs, the mail category, the mail class and subclass, indicators as to whether the receptacle is the highest numbered in the despatch, whether it contains registered or insured mail, and the gross weight.

The label containing the barcode is probably the single most important UPU form for ensuring quality of service [2, 8]. The UPU Postal Transport Guide describes the contents of the 29-character receptacle-ID [8]. The use of color is an important element of receptacle labels. The colors in most common use are [2]

- Parcel Post: yellow ochre
- EMS: blue/orange striped
- Empty bags : green

- Ordinary Letter Post: white, blue, red (white for priority; blue for non-priority; red for registered and insured items)
- Bulk Letter Post: violet, red

In addition, every country has a different receptacle bag color.

Each receptacle is a component of one and only one postal despatch. All receptacles in a specific despatch have the same origin IMPC, destination IMPC, mail category, class, subclass, despatch year, despatch number, and planned means of transportation (but the actual means of transportation can differ). Despatches, which are sequentially numbered within a despatch series, are established between the origin IMPC and the destination IMPC. The despatch number is reset by each IMPC at the beginning of the calendar year. Each despatch is accompanied by (defined by) a letter or parcel Bill (CN 31 Letter Bill, CN 32 Letter Bill Bulk Mail, and CP 87 Parcel Bill) describing the despatch and number of receptacles. A despatch can consist of one or many receptacles, depending on the volume of mail at the time [2].

Receptacles are included in consignments for transport purposes. A consignment consists of one or more receptacles assigned to a specific transport (for example, a specific air carrier flight). Each consignment is accompanied by (defined by) a delivery Bill (CN 37 Surface mails, CN 38 Airmails, and CN 41 Surface airlifted (S.A.L.) mails). Receptacles of a despatch may not all travel together. And they may not travel on the same transport that was planned when the despatch was created. Receptacles of several different despatches may travel on a specific transport as shown in Figure 2 [2, 4, 8].

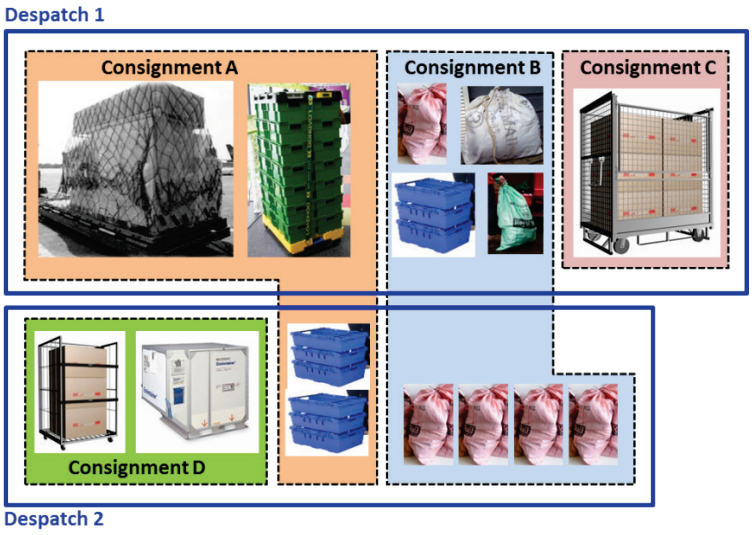

Figure 2: Relationship of Receptacles (Bags, Cans, Containers, ULDs), Despatches, and Consignments

Inbound International Mail

Once inbound international mail is received at a destination IMPC, it must be properly processed. Postal items are separated by mail category, class, and subclass; sorted; and screened, including by national Customs personnel and systems.

Transshipment and Transit Mail

Specific handling (and thus specific controls) is required for mail that is being transported from an origin OE (office of exchange) to a destination OE but may be temporarily stored at one or more intermediate airports during its transportation lifecycle. This mail is referred to as transshipment or transit mail. Several IMPCs are in "hub" countries where daily direct air transport is readily available to many destinations. But many IMPCs are in "spoke" countries, where transshipment or transit is required for most destinations. These are defined as follows [2, pp. 19-24 with diagrams]:

- Transshipment mail: mail that is enroute from one country to another and passes through an intermediate (third party) country. Such mail remains in the intermediate country's Airport Operations Area (AOA). Direct transshipment intraline is a transfer from one flight to another where both flights are operated by the same carrier (higher probability of success). Direct transshipment interline is a transfer from one flight to another where the flights are operated by different carriers, requiring careful planning and coordination.
- Transit Mail: mail that is staged and reprocessed at the IMPC of the transit (intermediate/third party) country. Such mail involves at least two airlines and two sets of ground handlers. Transit mail is designated as closed transit or open transit as follows:
  - Closed Transit: The origin OE's receptacle is not opened and is included in a consignment created by the transit Post at the Airmail Unit, as shown in Figure 3. Such mail involves the Airmail Unit of an IMPC but does not involve an OE. Closed transit is used when mail volumes warrant a closed despatch but the origin IMPC is not in a position to effectively plan the transportation all the way to the destination.
  - Open Transit: The origin OE's receptacle is opened and mail from the transit Post is added in a new despatch created by transit Post at the OE. Such mail involves the Airmail Unit of the IMPC and the OE. Open transit is used when mail volumes do not warrant a closed despatch.

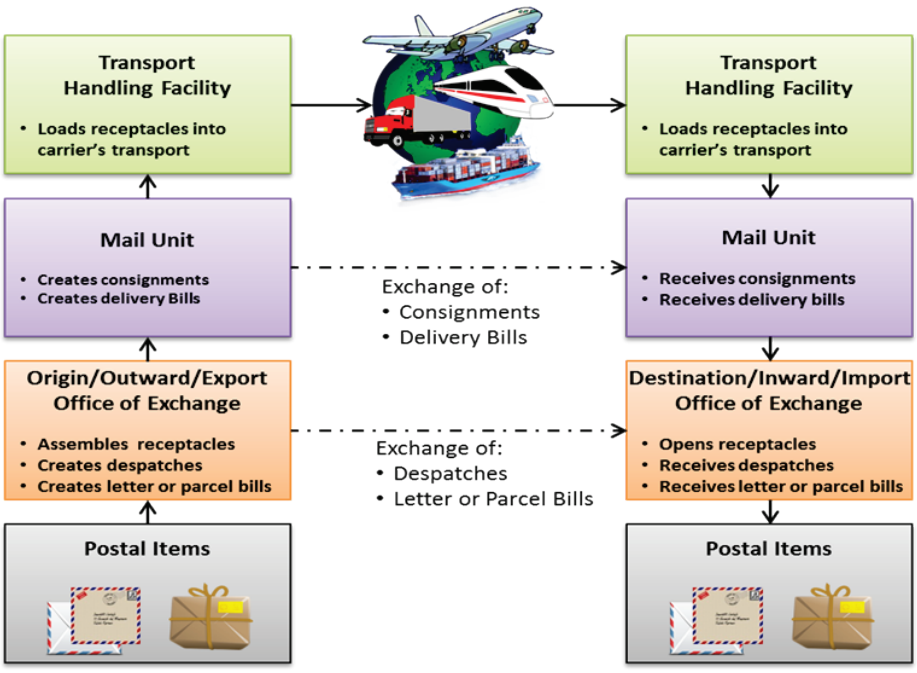

Figure 3: Relationships and Roles of OEs, Mail Units, and Handling Facilities

Transportation Systems

A number of distinct systems are used to ensure that international mail is effectively and accurately processed and transported. The specific systems vary by country but typically provide the following functional capabilities:

- Parcel sortation
- Receipt verification for inbound mail
- Scanning systems for mail visibility
- Customs processing (into Customs, out of Customs)
- Assigning receptacles to specific air carrier flights and despatches and receptacle receipt and reconciliation. One example is the CAPE (Computer Aided Post through EDI) system used by national Posts for scanning, assigning receptacle-IDs, assigning consignments, and tracking.
- Export control and other types of inspections
- Alerting systems, which can be used to stop processing

All of these systems require adequate controls, continuous monitoring, and regular maintenance to ensure they are performing as expected.

Refer to the CERT-RMM Technology Management process area for further details on specifying, acquiring, installing, monitoring, and maintaining systems that are used to process international mail.

For both outbound and inbound mail, potential and confirmed violations of UPU standards are identified as discrepancies and assigned to appropriate national Posts and other authorities for further handling.

IMT:SG2.SP1 Process Outbound International Mail

Outbound international mail is processed for transportation in accordance with standards.

The processing of outbound international mail begins when the mail has been successfully inducted by a national postal administration and transported to the origin IMPC, as shown in Figure 1. When postal items arrive at the IMPC, they are separated by mail category, class, and subclass, sorted by country, and screened (including Customs and export control screens if required). Postal items are assigned to receptacles, and receptacles are assigned to despatches and consignments. Consignments are assigned to a specific transport (for example, air carrier and flight) for transportation to the destination IMPC. The departure of consignments from the IMPC completes outbound processing and is the starting point for IMT:SG2.SP2, Transport Outbound International Mail.

Applicable UPU standards may include the *Letter Post Manual* [4], the *Parcel Post Manual* [5], the *Postal Transport Guide* [2], the *Transport Service Agreement template* [9], S58 [6], and S59 [7]. (Refer to IMT:SG1.SP1 for additional guidance about standards.)

Refer to IMT:SG5, Manage International Mail Discrepancies During Transportation, for the handling of discrepancies identified during the processing of outbound international mail.

Typical Work Products

1. Sorted mail
2. Screened mail
3. Receptacles
4. Despatches
5. Consignments

Subpractices

1. Sort mail.

   Postal items are sorted based on UPU standards and the required postal administration standards and sortation schemes. Typical schemes for sortation include by postal item category, class, subclass, dimensions, weight, packaging, destination country, IMPC, and postcode/delivery zone.

2. Screen mail.

   Postal items are screened in accordance with UPU and postal administration standards. Examples of S59 [7] screening standards for outbound mail intended for carriage on passenger aircraft include the following:

   - Screening methods (use one or more of the following):
     - hand search/visual inspection
     - X-ray equipment (prohibited for use by the USPS)
     - explosive detection system (EDS)

    - explosive detection dog (EDD)
    - explosive trace detection (ETD)
  - High-risk items (such as dangerous and hazardous goods and evidence of tampering) are required to undergo additional screening.
  - Screening equipment should be maintained, tested, and operated in accordance with the manufacturer's instructions.
  - All personnel conducting screening are properly trained and supervised.

  Postal items exempt from screening are identified in S59.

  Upon request, outbound mail is screened by Customs. Postal items are scanned going into Customs screening and are scanned when they exit Customs screening. Screened mail may be placed on hold by Customs Agents. Held mail is identified as a discrepancy (refer to IMT:SG5.SP2).

  Outbound mail is screened in accordance with national and postal administration export control standards. Screened mail may be placed on hold by export control inspectors. Held mail is identified as a discrepancy (refer to IMT:SG5.SP2).

3. Assign postal items to receptacles.

   Postal items are assigned and loaded into receptacles (typically country color-coded bags) in accordance with standards (such as the *UPU Postal Transport Guide* [2]) and sortation schemes. Each receptacle is given a unique ID and label as described in the *UPU Postal Transport Guide* and may be scanned to generate EDI messages. Oversized postal items that do not fit into receptacles are transported separately as outside pieces and given a unique receptacle-ID.

4. Assign receptacles to despatches.

   Receptacles are assigned to despatches (for example, based on their origin IMPC, destination IMPC, and mail category, class, and subclass) in accordance with standards (such as the *UPU Postal Transport Guide* [2]). Each despatch has a unique ID, which is sequentially numbered with a despatch series. Each despatch is accompanied by documentation describing the despatch and its number of receptacles and may be scanned to generate EDI messages.

5. Assign receptacles to consignments.

   Receptacles are assigned to consignments (for example, all receptacles for a specific transport such as a specific air carrier flight) in accordance with standards (such as the *UPU Postal Transport Guide* [2]). Receptacles are assigned to flights by weight and typically placed in "cans," which are also referred to as containers and ULDs. Each container has a unique barcode and is sealed. If all receptacles in a container have the same destination, they are scanned with the container barcode (referred to as nested containers). This process is not used if the receptacles in that container have multiple destinations.

Each consignment has a unique ID, is accompanied by documentation, and may be scanned to generate EDI messages. A postal administration sends consignment information to the receiving air carrier in advance so that they can plan their aircraft loads.

During the assignment of receptacles to specific transports, routes for such transportation are optimized to ensure timely delivery and address identified risks and other factors that affect routing, such as weather, civil unrest, and the availability of destination IMPCs to accept the consignment. That said, while UPU regulations encourage using the most direct route, even when direct routes are available, IMPCs may choose less-direct routes if the service requirements can be met and if they are more cost-effective.

Receptacles may be held for several days if flights are not available (for example, flights from the U.S. to Russia).

IMT:SG2.SP2 Transport Outbound International Mail

Outbound international mail is transported to destination processing facilities in accordance with standards.

The transportation of outbound international mail begins when a mail consignment is picked up from the outbound IMPC and transported to the air carrier facility or warehouse. For an air carrier, the Delivery Bill and UPU standard receptacle labels define a shipment as being mail rather than cargo or freight and enable the airline processes relating to mail to be applied.

Consignments are processed at the air carrier facility as required by national law, UPU standards, and air carrier procedures and then transported to the specific flight for transportation to the destination IMPC. A consignment may be transported directly on one flight or may be temporarily held at an intermediate airport and/or IMPC awaiting its next flight. If the latter is the case, the consignment is handled as transshipment mail or transit mail, both of which require additional controls as described in IMT:SG5.

Transshipment mail may pass through one or more intermediate countries while enroute and remains in the intermediate country's Airport Operations Area (AOA) (i.e., it remains in the custody and control of the AOA air carrier).

Transit mail is staged and reprocessed at the IMPC of the intermediate country (with all of the requisite handoffs between the air carrier and the IMPC). (Refer to IMT:SG4.SP4 for details about controlling custody of mail.) For transit mail that is designated as closed, the origin receptacle is not opened and is included in a new consignment created by the transit country's IMPC. The despatch and despatch series for this receptacle remain the same. For transit mail that is designated as open, the origin receptacle is opened and mail from the transit country's IMPC is added, creating a new despatch (that may be part of a new despatch series) and a new consignment (*refer to IMT:SG2.SP1*).

Applicable UPU standards may include the *Letter Post Manual* [4], the *Parcel Post Manual* [5], the *Postal Transport Guide* [2], and the *Transport Service Agreement template* [9]. *(Refer to IMT:SG1.SP1 for additional guidance about standards.)*

Risks that may arise when mail is being transported from the IMPC to the air carrier facility and from that facility to the aircraft are described in IMT:SG3, Manage Risks to International Mail During Transportation.

Refer to IMT:SG5, Manage International Mail Discrepancies During Transportation, for the handling of discrepancies identified during the transportation of outbound international mail.

Typical Work Products

1. Consignments transported to air carrier facility
2. Consignments processed at air carrier facility
3. Consignments loaded onto specific aircraft
4. Transshipment receptacles
5. Transit receptacles
6. Evaluations of air carrier provider performance

Subpractices

1. Transport consignments from the origin IMPC to the air carrier facility.

   Consignments may be transported via truck, airline transportation equipment, and other means by postal administration, airline, and service contractor personnel.

2. Process consignments at the air carrier facility.

   Processing that occurs at an air carrier facility includes scanning and may include additional screening required by national and international laws. Carrier communication with the origin and destination IMPCs may be supported by EDI messaging (refer to IMT:SG4.SP5).

   If containers arrive that are not full, they are left open in a secure area so that they can be filled with additional mail if possible.

3. Consignments are loaded onto trucks, airline transportation equipment, ULDs, or other transports by airline or service contractor personnel.

4. Transport and load consignments onto the assigned aircraft and flight.

   Airline and service contractor personnel check all container seals before mail is loaded onto the aircraft and notify the airline if any seal is broken (which would be handled as a discrepancy).

5. Transport consignments (enroute flights).

Consignments are transported from the air carrier facility at the origin country to the air carrier facility at the destination country.

6. Process transshipment receptacles.

   A receptacle designated as transshipment mail remains in the transit country's AOA and is loaded onto its next scheduled aircraft and flight.

7. Process transit receptacles.

   A receptacle designated as closed transit mail is transported by the air carrier to the transit country's IMPC. It is included in a new consignment created by the IMPC. The container is handed off to the air carrier and loaded onto its scheduled aircraft and flight.

   A receptacle designated as open transit mail is transported by the air carrier to the transit country's IMPC. The receptacle is opened and postal items from the transit country's IMPC are added, creating a new despatch and a new consignment. The container is handed off to the air carrier and loaded onto its scheduled aircraft and flight.

8. Monitor and evaluate the performance of air carrier providers in accordance with executed contracts.

   Air carriers (and their service contractors, if this is in scope) are continuously monitored and periodically assessed or evaluated to ensure that they are providing all services, at the stated service levels, and meeting all of the terms and conditions of their contracts with the respective IMPC.

   In addition, air carrier providers (and their service contractors, if this is in scope) are required to demonstrate compliance with UPU standards (for example, S58 Section 6, "Personnel security and training").

   Ensuring that resilience requirements for postal items are met by service contractors and other external entities involved during transportation is addressed in the CERT-RMM External Dependencies Management process area.

IMT:SG2.SP3 Transport Inbound International Mail

Inbound international mail is transported to destination processing facilities in accordance with standards.

The transportation of inbound international mail begins when a mail consignment arrives at the destination airport. It is unloaded from the aircraft and transported to the air carrier facility. Mail is loaded onto trucks or other transports, transported to the destination IMPC, and scanned by the air carrier.

Applicable UPU standards may include the *Letter Post Manual* [4], the *Parcel Post Manual* [5], the *Postal Transport Guide* [2], the *Transport Service Agreement template* [9], and S58 [6]. (Refer to IMT:SG1.SP1 for additional guidance about standards.)

Refer to IMT:SG5, Manage International Mail Discrepancies During Transportation, for the handling of discrepancies identified during the transportation of inbound international mail.

Ensuring that resilience requirements for postal items are met by service contractors and other external entities involved during transportation is addressed in the CERT-RMM External Dependencies Management process area.

Typical Work Products

1. Consignments offloaded from specific aircraft
2. Consignments processed for transport at air carrier facility (inbound)
3. Consignments transported to destination IMPC
4. Evaluations of air carrier provider performance

Subpractices

1. Receive consignments at the destination airport and offload them from the aircraft.

   Consignments are offloaded from their aircraft and inspected to ensure that no discrepancies have occurred enroute, in transshipment, or in transit.

2. Consignments are loaded onto trucks, airline transportation equipment, ULDs, or other transports by airline or service contractor personnel.
3. Transport consignments to the destination IMPC and perform air carrier scan.

   Consignments may be transported by postal administration, airline, or service contractor personnel. The air carrier scans all containers (at the air carrier facility or the IMPC), which transfers custody to the IMPC.

4. Monitor and evaluate the performance of air carrier providers in accordance with executed contracts.

   Air carriers (and their service contractors, if this is in scope) are continuously monitored and periodically assessed or evaluated to ensure that they are providing all services, at the stated service levels, and meeting all of the terms and conditions of their contracts with the respective IMPC.

   In addition, air carrier providers (and their service contractors, if this is in scope) are required to demonstrate compliance with UPU standards (for example, S58 Section 6, “Personnel security and training” [6]).

IMT:SG2.SP4 Process Inbound International Mail

Inbound international mail is processed in accordance with standards.

The processing of inbound international mail begins when the mail has been received at the IMPC. Receptacles are opened and postal items are scanned and screened as required by standards and national laws. Applicable UPU standards may include the *Letter Post Manual* [4], the *Parcel Post Manual* [5], the *Postal Transport Guide* [2], the *Transport Service*

Agreement template [9], and S58 [6]. (Refer to IMT:SG1.SP1 for additional guidance about standards.)

IMPCs may set timeliness (availability) goals for mail processing, such as ensuring that all mail that is received by noon will be out by midnight, or if received after noon, by midnight the next day.

Refer to IMT:SG5, Manage International Mail Discrepancies During Transportation, for the handling of discrepancies identified during the processing of inbound international mail.

Typical Work Products

1. Mail received at IMPC
2. Entry scans
3. Screened mail

Subpractices

1. Receive mail.

   The IMPC takes possession and custody of the mail despatch from the air carrier at the IMPC receiving area.

2. Scan mail.

   Receptacles are opened, and an entry or possession scan is performed using a Receipt Verification System or other means.

   Postal clerks may flag packages for inspection or for referral to a supervisor for other review.

   Trackable items such as EMS may be scanned individually to confirm arrival at the destination IMPC.

3. Screen mail.

   All inbound mail must pass through a radiation portal operated by Customs.

   Postal inspectors may review letters for illegal activity such as lottery mail and hold suspicious mail for further investigation.

   If damage to a postal item is discovered when postal items are being handed off to Customs, it is treated as a discrepancy.

   Customs performs a Customs In scan of inbound mail and conducts further screening, such as X-ray screening. Customs may hold suspicious mail and pass it to Postal inspectors for review. Once mail has been cleared by Customs, it is given an Out of Customs scan.

IMT:SG3 Manage Risks to International Mail During Transportation

Operational risks to international mail during transportation are identified and addressed.

The management of risk for mail is the specific application of risk management tools, techniques, and methods to mail that is accepted, processed, transported, and delivered by a postal administration. Due to the high volume of mail, the extensive geography over which it is delivered, and the number of organizations and individuals that participate in the mail process, there are many opportunities for postal items to be threatened and for risks to be realized throughout the mail lifecycle, including damage, theft, loss, and fraud. Realized risk can result in indemnity claims, loss of market share, loss of revenue, harm to the reputation of the postal administration, shutting down the postal administration, and other consequences.

Managing operational risks to mail involves determining where vulnerabilities and threats to mail arise and where mitigation controls must be implemented to protect postal items from violations of their resilience requirements—access, availability, sanctity, custody, and visibility. Mail risk categories include, for example,

- locations where postal items physically reside (receptacles (cans, containers), facilities, docks, airplanes, trucks, trains, ships, etc.). This includes risk at origin, destination, and delivery locations and facilities where mail may be delayed or it may be unsafe to deliver mail due to potential but unpredictable disruptive events (such as fires, explosions, and civil unrest), as well as disruptive events that occur with some periodicity and predictability (such as hurricanes and winter storms).
- mail in the custody of service providers such as air carriers, including mail in transshipment and transit status
- dangerous and hazardous mail
- mail aggregations (single items, receptacles, despatches, and consignments)
- automation used in processing mail (for example, sorting, scanning, and screening technologies)
- personnel (postal administration employees, mailers, service providers and contractors, airline and other transportation personnel, etc.)
- mail under investigation, including airline crashes and delays
- target countries where risks to mail are known to be high

The identification and mitigation of risks to the successful collection of mail revenue are addressed in the CERT-RMM Mail Revenue Assurance process area.

IMT:SG3.SP1 Identify and Assess Risks to International Mail During Transportation

Operational risks to international mail during transportation are periodically identified and assessed.

Risks that can affect mail must be identified and assessed in order to actively manage the resilience of postal items and ensure that they reach their destination as intended by the

mailer, the participating postal administrations, and in accordance with mail transportation standards. The identification of risks to mail forms a baseline from which a continuous risk management process can be established and managed.

The subpractices included in this practice are generically addressed in goals RISK:SG3 and RISK:SG4 in the CERT-RMM Risk Management process area.

Typical Work Products

1. Postal item risk statements, with impact valuation
2. List of postal item risks, with categorization and prioritization

Subpractices

1. Determine the scope of the risk assessment for mail.

   Determining which mail (category, class, subclass, supplementary services, origin, destination, etc.) to include in regular risk management activities depends on many factors, including the value of the postal items to the postal administration and its resilience requirements.

2. Identify risks to postal items.

   Identification of risk for postal items requires an examination of all the places where mail is physically located from induction to delivery. Risks should be identified in these contexts so that mitigation and control actions are more targeted.

   These are examples of operational risks for mail:

   - hazardous and dangerous materials
   - theft of cash from postal items by service contractors while loading mail into an aircraft
   - inadvertent loss of postal items during transport between the IMPC and air carrier contractor facility
   - damage to mail resulting from failure to protect it from exposure to weather during rampside transport
   - tampering resulting from access to a loading dock by unauthorized persons
   - destruction from fire, natural disaster, or aircraft crash
   - originating from or destined for high-risk countries
   - vulnerabilities in technologies that support the transportation of mail
   - gaps between standards and the controls in place to meet them

3. Analyze risks to postal items.

   Risk analysis includes determining, as accurately as possible, the likelihood, consequences, and potential impact of each risk.

4. Categorize risks to postal items according to the defined risk categories, and prioritize risks for disposition and mitigation.

5. Assign a risk disposition to each postal item risk.

   Examples of risk dispositions are “accept,” “transfer,” “research,” and “mitigate” (or “control”).

6. Monitor the risk and the risk strategy on a regular basis to ensure that the risk does not pose additional threat to the sanctity of mail.

7. Develop a strategy for risks that the postal administration decides to mitigate.

IMT:SG3.SP2 Address Risks to International Mail During Transportation

Identified operational risks to international mail during transportation are addressed.

The mitigation of risks to mail involves the development of strategies that seek to minimize the risk to an acceptable level. This includes reducing the likelihood of risks to postal items, minimizing exposure to risks, developing service continuity plans to keep postal items viable during times of disruption, and developing recovery and restoration plans to address the consequences of realized risk.

Risk mitigation for postal items requires the development of risk mitigation plans (which may include the development of new mail resilience controls or revision of existing controls) and implementing and monitoring these plans for effectiveness.

The subpractices included in this practice are generically addressed in goal RISK:SG5 in the CERT-RMM Risk Management process area.

Typical Work Products

1. Postal item risk mitigation plans
2. List of those responsible for addressing and tracking risks
3. Status on postal item risk mitigation plans

Subpractices

1. Develop and implement risk mitigation strategies for all risks that have a “mitigate” or “control” disposition.

   For example, a strategy to mitigate vulnerabilities in technologies that support the transportation of mail would be to regularly perform vulnerability scanning, analysis, and resolution on those technologies. (Refer to the CERT-RMM Vulnerability Analysis and Resolution process area for more information.)

2. Validate the risk mitigation plans by comparing them to existing strategies.
3. Identify the person or group responsible for each risk mitigation plan and ensure that they have the authority to act and the proper level of skills and training to implement and monitor the plan.
4. Address residual risk.

5. Implement the risk mitigation plans and provide a method to monitor the effectiveness of these plans.
6. Monitor risk status.
7. Collect performance measures on the risk management process.

IMT:SG4 Control International Mail During Transportation

Controls to protect international mail during transportation are established and maintained in accordance with standards.

A control is a policy, procedure, method, technology, or tool that satisfies a stated objective. Controls for the protection of international mail during transportation should meet objectives for quality of service, mitigation of risks identified through risk assessment, and resilience requirements. These controls should also meet objectives for compliance to related standards, such as S58 access control standards, S59 screening standards, the *Letter Post Manual* [4], the *Postal Transport Guide* [2], and *Regulations of the EMS Standard Agreement*. (Refer to IMT:SG1.SP1 for additional guidance about standards.)

Controls can be broad and general or specific and targeted. Broad controls typically apply universally to all processes that can affect aspects of the transportation of mail.

Controls can be administrative, technical, or physical. Administrative controls ensure alignment to postal administration management's intentions and include such actions as governance, setting policy, monitoring, auditing, and performance measurement. Technical controls are implemented through technology means. They typically exist in automated processes, manifested in software, hardware, devices, systems, and networks. Physical controls provide physical barriers to access that typically apply to people, containers, and facilities.

The specific practices in this goal provide guidance for establishing controls for assuring access to and the availability, sanctity, custody, and visibility international mail during transportation as required by UPU standards and national and international standards and laws. Note that some controls may fulfill multiple resilience requirements. For example, the same physical access controls might be used both to prevent theft (availability) and prevent tampering (sanctity).

Refer to the CERT-RMM Human Resource Management process area for a description of candidate controls regarding the performance and integrity of postal administration personnel where such performance and integrity may affect the protection of international mail during transportation (resilience as a job responsibility, for example).

Refer to the CERT-RMM People Management process area for a description of candidate controls regarding the availability of postal administration personnel to perform international mail transportation (ensuring the availability of trained backup staff during disruptive events, for example).

Refer to the CERT-RMM Organizational Training and Awareness process area for a description of candidate controls regarding the preparedness and readiness of postal administration personnel to perform international mail transportation activities (adequate training, for example).

Refer to the CERT-RMM Measurement and Analysis process area for more information about establishing metrics to evaluate the effectiveness of controls.

Refer to the CERT-RMM Monitoring process area for more information about the collection, organization, and distribution of data that may be useful in determining the effectiveness of controls.

IMT:SG4.SP1 Control Access to International Mail During Transportation

Controls are established and maintained to assure access to international mail during transportation in accordance with standards.

Access is the authorized ability, right, or privilege of a person or system to sort, scan, screen, view, or take physical possession of a postal item. Access thus affects all other resilience requirements—availability, sanctity, custody, and visibility. A foundational aspect of the resilience of international mail during transportation is ensuring that only authorized persons have access to mail and only to the extent to which they have been authorized.

The appropriate level of access control should be implemented in mail conveyance vehicles, postal facilities and contract facilities, temporary holding areas, loading areas, EDI systems, and any other place where mail or mail transport information is handled, stored, or processed [6].

Administrative access controls include access and security policies, background screening of employees and service contractors, and access lists for service contractors showing specific days on site and work being performed. Technical and technical/physical controls include access control lists in application systems and databases, key card and key pad readers for facilities, surveillance cameras, and using badge readers to restrict access to certain areas of a facility. Regardless of the method used, access controls must adequately screen and differentiate the access privileges of employees, visitors, and service contractors at all points of access to mail and mail-processing systems [6]. Examples of physical controls include using fixed security guard posts to verify the identities of individuals entering or leaving secure areas, requiring individual badges for and escorts for visitors, using barbed wire fences around critical facility perimeters, and locking facility doors and windows. *(See IMT:SG4.SP2 and IMT:SG4.SP3 for examples of access controls that address availability and sanctity requirements.)*

The selection, implementation, and management of access controls and the association of privileges to identities are performed in the CERT-RMM Access Management process area.

The selection and implementation of appropriate access controls for facilities is performed in the CERT-RMM Environmental Control process area.

The creation, maintenance, and deprovisioning of identities representing persons who require access to mail are addressed in the CERT-RMM Identity Management process area.

Typical Work Products

1. Mail access controls (including the responsible party)
2. Traceability matrix of standards, policies, operating procedures, and other specifications and mail access controls
3. Mail access control gaps
4. Mail access control updates
5. Discrepancies identified by mail access controls

Subpractices

1. Establish and implement mail access controls in accordance with standards.
2. Confirm or assign responsibility for implementing access controls.

   Confirmation is required for existing and updated controls. Assignment is required for new controls.
3. Develop a bidirectional traceability matrix that maps standards and controls.
4. For standards that are not addressed by controls, identify and manage the risks associated with control gaps as described in IMT:SG3, Manage Risks to International Mail During Transportation.
5. Regularly review and assess the effectiveness of controls and update or retire controls as needed.

   As standards, services, processes, and technologies change, gaps and redundancies may arise between mail access standards and the controls established to satisfy them. *(Refer to CERT-RMM CTRL:SG4.SP1 for further information about periodically assessing and adjusting controls.)*
6. Identify discrepancies identified by mail access controls.

   Refer to IMT:SG5, Manage International Mail Discrepancies During Transportation, for the handling of discrepancies identified by mail access controls.

IMT:SG4.SP2 Control Availability of International Mail During Transportation

Controls are established and maintained to assure availability of international mail during transportation in accordance with standards.

Availability is the requirement that postal items be accessible to all authorized personnel in a timely fashion as determined by the mail category, class, and subclass. To achieve that requirement, mail must not be lost, stolen, or unnecessarily delayed. Once mail enters the mailstream, it must follow normal processing and transfer sequences and service standards.

It must not be removed from the mailstream except as allowed by laws and standards, such as in S59 Section 5.6, where a consignment can be rejected if screening processes fail to reasonably establish that it does not contain dangerous goods. *(See IMT:SG2.SP1 and IMT:SG2.SP4 for information regarding screening processes.)*

Mail availability controls should satisfy national and international laws, standards, policies, operating procedures, and other specifications that relate to and affect the availability of mail, provide confidence that they are being followed, and reduce the risks that would result in mail being unavailable.

Administrative controls for limiting delay of mail might include capacity management plans, alternate routes, limiting how long postal items may be held at a contractor facility before they must be returned to the IMPC, and penalties for missent mail. Examples of administrative controls for detecting possible loss or theft are using sequential despatch numbers and identifying on the Letter or Parcel Bill the number of receptacles despatched. Examples of technical controls are closed circuit television systems, electronic card access control systems, and using a volume production alert system to identify allocation issues early in the production process and trigger remedial action prior to the consignment closure [11, FBP02-07]. *(See IMT:SG4.SP1 for more details about access controls.)* Physical controls for mail availability include picture IDs, locks used to secure collection and relay boxes, facility alarm systems, and locks and numbered tin band seals on trucks that are transporting mail. Blue and orange striped receptacle labels are used to distinguish EMS mail. Perimeter fences and adequate lighting systems are physical measures taken to help prevent robbery in open areas [6, Section 5.1].

A broad availability control might be an organizational culture of concern for and commitment to promptness. Specific availability controls may be applied to certain mail products, such as insurance against loss for Parcel Post. They also include in-process controls that happen at specific points in the mailstream lifecycle. For example, item scans on arrival at the destination IMPC affirm that EMS and other trackable postal items are still in the mailstream and show whether they've been delayed.

The subpractices included in this practice are generically addressed in the CERT-RMM Controls Management process area.

Typical Work Products

1. Mail availability controls (including the responsible party)
2. Traceability matrix of standards, policies, operating procedures, and other specifications and mail availability controls
3. Mail availability control gaps
4. Mail availability control updates
5. Discrepancies identified by mail availability controls

Subpractices

1. Establish and implement mail availability controls in accordance with standards.
2. Confirm or assign responsibility for implementing availability controls.

   Confirmation is required for existing and updated controls. Assignment is required for new controls.
3. Develop a bidirectional traceability matrix that maps standards and availability controls.
4. For standards that are not addressed by availability controls, identify and manage the risks associated with control gaps as described in IMT:SG3, Manage Risks to International Mail During Transportation.
5. Regularly review and assess the effectiveness of availability controls and update or retire controls as needed.

   As standards, services, processes, and technologies change, gaps and redundancies may arise between mail availability standards and the controls established to satisfy them. (Refer to CERT-RMM CTRL:SG4.SP1 for further information about periodically assessing and adjusting controls.)
6. Identify discrepancies identified by mail availability controls.

   Refer to IMT:SG5, Manage International Mail Discrepancies During Transportation, for the handling of discrepancies identified by mail availability controls.

IMT:SG4.SP3 Control Sanctity of International Mail During Transportation

Controls are established and maintained to assure sanctity of international mail during transportation in accordance with standards.

Sanctity is the requirement that postal items be protected from damage, alteration of original content, disclosure, and destruction. It includes the principle of the "sanctity of the seal" for certain classes of mail, which protects such postal items against unauthorized access to their contents. Sanctity encompasses the information resilience requirements of integrity (keeping the asset in the condition intended by the owner) and confidentiality (ensuring that the asset is accessible only to authorized people, processes, and devices) for postal items.

Mail sanctity controls should satisfy national and international laws, standards, policies, operating procedures, and other specifications that relate to and affect the sanctity of mail, provide confidence that they are being followed, and reduce the risks that would result in mail sanctity being violated.

Administrative controls for sanctity include response procedures for suspicious mail incidents, background screening on personnel consistent with national legislation, and maintaining a process to report employee misconduct [6, Section 6.2]. Technical controls for mail sanctity include surveillance cameras, metal detectors, and X-ray screening to detect dangerous goods. *(See IMT:SG2.SP1 and IMT:SG2.SP4 for information regarding screening*

processes.) Physical controls for mail sanctity include physical segregation of dangerous goods and shrink-wrapping of containers. Controls that protect mail against theft, such as using locking mechanisms and key controls [6, Section 5.1.6] also serve to protect mail against unauthorized access with the intent of disclosure or destruction. *(See IMT:SG4.SP1 for more details about access controls.)*

Broad controls that can affect the sanctity of mail include postal administration standards of conduct that are impressed upon employees by supervisors and sustained by the influence of the culture. Specific sanctity controls include in-process controls that happen at specific points in the mailstream lifecycle, such as visual inspection of receptacles at the air carrier facility and at the aircraft.

The subpractices included in this practice are generically addressed in the CERT-RMM Controls Management process area.

Typical Work Products

1. Mail sanctity controls (including the responsible party)
2. Traceability matrix of standards, policies, operating procedures, and other specifications and mail sanctity controls
3. Mail sanctity control gaps
4. Mail sanctity control updates
5. Discrepancies identified by mail sanctity controls

Subpractices

1. Establish and implement mail sanctity controls for postal items in accordance with standards.
2. Confirm or assign responsibility for implementing sanctity controls.

   Confirmation is required for existing and updated controls. Assignment is required for new controls.
3. Develop a bidirectional traceability matrix that maps standards and sanctity controls.
4. For standards that are not addressed by sanctity controls, identify and manage the risks associated with control gaps as described in IMT:SG3, Manage Risks to International Mail During Transportation.
5. Regularly review and assess the effectiveness of sanctity controls and update or retire controls as needed.

   As standards, services, processes, and technologies change, gaps and redundancies may arise between mail sanctity standards and the controls established to satisfy them. (Refer to CERT-RMM CTRL:SG4.SP1 for further information about periodically assessing and adjusting controls.)

6. Identify discrepancies identified by mail sanctity controls.

   Refer to IMT:SG5, Manage International Mail Discrepancies During Transportation, for the handling of discrepancies identified by mail sanctity controls.

IMT:SG4.SP4 Control Custody of International Mail During Transportation

Controls are established and maintained to assure custody of international mail during transportation in accordance with standards.

Custody is the state of postal items being in the immediate charge and control of authorized Post, carrier, and service contractor personnel from acceptance at the origin IMPC through delivery to the destination IMPC.

Custody controls should demonstrate the satisfaction of national and international laws, standards, policies, operating procedures, and other specifications that relate to and affect the custody of mail, provide confidence that they are being followed, and reduce the risks that would result in the inability to maintain the custody of postal items as required. Custody requirements may vary based on mail category, class, and subclass, such as insured mail and EMS.

Custody controls primarily relate to proof of acceptance, handover, and delivery of mail. Postal administrations must maintain direct custody (themselves or through their designees) and control of international mail intended for carriage by air from the time of acceptance until it is dispatched to a carrier, agent, or designee [7, pg. 3]. Mail is considered to be in the custody of the carrier from the carrier's proof of acceptance of a consignment until its handover at the destination or at the transit airport and the transmission of the associated proof of delivery [9, pg. 8].

Administrative custody controls include paper-based UPU consignment information, proof of acceptance or delivery through signed documents, and procedures for handover failures (if, for example, a carrier refuses a handover because the mail appears to be damaged) [2; 9, Article 5].

Technical controls include electronic messaging used to prove handovers, such as CARDIT messages sent to carriers for consignments handed over and RESDIT messages sent by carriers indicating receptacles have been handed over to the destination Post *(see IMT:SG4.SP5)*. These must be done in conformity with UPU EDI messaging standards [9].

Refer to IMT:SG2.SP2, Transport Outbound International Mail, and IMT:SG2.SP3, Transport Inbound International Mail, for further information about custody requirements.

Typical Work Products

1. Mail custody controls (including the responsible party)
2. Traceability matrix of standards, policies, operating procedures, and other specifications and mail custody controls
3. Mail custody control gaps

4. Mail custody control updates
5. Discrepancies identified by mail custody controls

Subpractices

1. Establish and implement mail custody controls in accordance with standards.
2. Confirm or assign responsibility for implementing custody controls.

   Confirmation is required for existing and updated controls. Assignment is required for new controls.
3. Develop a bidirectional traceability matrix that maps standards and custody controls.
4. For standards that are not addressed by custody controls, identify and manage the risks associated with controls gaps as described in IMT:SG3, Manage Risks to International Mail During Transportation.
5. Regularly review and assess the effectiveness of custody controls and update or retire controls as needed.

   As standards, services, processes, and technologies change, gaps and redundancies may arise between mail custody standards and the controls established to satisfy them. (Refer to CERT-RMM CTRL:SG4.SP1 for further information about periodically assessing and adjusting controls.)
6. Identify discrepancies identified by mail custody controls.

   Refer to IMT:SG5, Manage International Mail Discrepancies During Transportation, for the handling of discrepancies identified by mail custody controls.

IMT:SG4.SP5 Control Visibility of International Mail During Transportation

Controls are established and maintained to assure visibility of international mail during transportation in accordance with standards.

Visibility is the ability to track international mail from acceptance to delivery by means such as electronic mailing documentation, barcodes on postal items and containers, and in-process scanning while mail is in the postal network. As a resilience requirement, the primary focus for visibility is mission assurance—ensuring that every postal item is accurately transported from the origin IMPC to the destination IMPC. Visibility enables tracing (determination, from processing records, of the last known physical location and status of an item) and tracking (the recording of significant events in the processing and transportation of an item, in order to provide a historical record of such events and to support tracing of the item) [8].

Visibility may be accomplished through standard paper forms such as Letter Bills CN31, Parcel Bills CP87, and Delivery Bills CN38 and CN41, as well as receptacle labels and item lists. Increasingly, however, end-to-end international mail visibility is achieved through

barcode scanning, other computerized data entries, and the exchange of standard EDI messages [12, pg. 4].

Origin IMPCs create a 29-character receptacle-ID in barcoded format for receptacle labels. It is scanned by transit and destination postal administrations and carriers. By scanning the receptacle-ID, the dispatch-ID and the dispatch-series is automatically captured [2].

Barcode scanning and other computerized entries generate EDI messages such as the following from the M39 standard [13] at postal item, receptacle, and transport levels [12]:

- Post-Post EDI
  - PREDES (PRE-advice of DESpatch): origin Post sends destination Post information about a despatch
  - RESDES (RESponse to DESpatch pre-advice): destination Post confirms to origin Post arrival of the despatch
  - PRECON (PRE-advice of CONsignment): origin Post sends destination Post information about a consignment
  - RESCON (RESponse to CONsignment pre-advice): destination Post confirms to origin Post mail received from carrier
- Post-Carrier EDI
  - CARDIT (CARrier/Documents International Transport advice): origin Post sends carrier information about a consignment
  - RESDIT (RESponse to Documents International Transport advice): carrier sends origin Post the mandatory message that establishes Proof of Delivery of a consignment

The RESDES, RESCON, and RESDIT messages are typically based on scanning the receptacle-ID [2, pg. 20].

Visibility requirements may vary based on mail category, class, and subclass. In electronic tracking, a 13-character barcoded item ID is used on all international trackable items (e.g., registered letters, parcels, and EMS items) [2, pg. 22]. UPU Standard EMSEVT messages can be used to record events for individual barcoded postal items, such as arrival at origin IMPC, departure from destination IMPC, and arrival at delivery office.

Typical Work Products

1. Mail visibility controls (including the responsible party)
2. Traceability matrix of standards, policies, operating procedures, and other specifications and mail visibility controls
3. Mail visibility control gaps
4. Mail visibility control updates
5. Discrepancies identified by mail visibility controls

Subpractices

1. Establish and implement mail visibility controls in accordance with standards.
2. Confirm or assign responsibility for implementing visibility controls.

   Confirmation is required for existing and updated controls. Assignment is required for new controls.
3. Develop a bidirectional traceability matrix that maps standards and controls.
4. For standards that are not addressed by controls, identify and manage the risks associated with control gaps as described in IMT:SG3, Manage Risks to International Mail During Transportation.
5. Regularly review and assess the effectiveness of controls and update or retire controls as needed.

   As standards, services, processes, and technologies change, gaps and redundancies may arise between mail visibility standards and the controls established to satisfy them. (Refer to CERT-RMM CTRL:SG4.SP1 for further information about periodically assessing and adjusting controls.)
6. Identify discrepancies identified by mail visibility controls.

   Refer to IMT:SG5, Manage International Mail Discrepancies During Transportation, for the handling of discrepancies identified by mail visibility controls.

IMT:SG5 Manage International Mail Discrepancies During Transportation

Discrepancies during the transportation of international mail are identified and addressed.

As stated in IMT:SG1.SP1, Establish Standards for Mail Transportation, mail transportation standards define what material can be transported and in what manner it can be transported—and therefore what postal administrations can accept for origin processing and destination processing. Non-compliance with these standards constitutes a mail discrepancy.

Non-compliance with standards for access to mail and the availability, sanctity, custody, and visibility of mail (refer to IMT:SG1.SP1) should also result in the identification of a mail discrepancy.

Mail discrepancies result from intentional and fraudulent acts and inadvertent omission or error. Discrepancies may be caused by mailers, postal administration personnel or systems, suppliers and contractors, or people using the mail to perpetrate criminal activity. Mail discrepancies can be innocuous and go unnoticed or can significantly impact the ability of a postal administration and the UPU to fulfill its mission. To ensure the operational resilience of the mail that it accepts, a postal administration must maximize its opportunities to identify discrepancies before mail is formally inducted. However, because not all mail

discrepancies can be prevented, a postal administration must have the capability to identify mail discrepancies during origin outbound processing, inbound and outbound transportation, and inbound destination processing and respond appropriately as defined in this specific goal. (*The management of mail discrepancies during induction is addressed in the CERT-RMM Mail Induction process area. The management of mail revenue discrepancies and mail revenue fraud is discussed in the CERT-RMM Mail Revenue Assurance process area.*)

In order to effectively resolve mail discrepancies, a postal administration must develop and maintain plans for managing mail discrepancies (identify, analyze, open an investigation, resolve, etc.), including having a structure and supporting systems for discrepancy event detection, reporting, logging, and tracking, and for collecting and storing discrepancy evidence.

The analysis of mail discrepancy events, their declaration as incidents, and the appropriate postal administration response are addressed in the CERT-RMM Incident Management and Control process area.

IMT:SG5.SP1 Establish and Maintain International Mail Discrepancy Plans for Transportation

Plans and procedures for managing discrepancies during the transportation of international mail are established and maintained.

A postal administration must develop plans and procedures for handling mail discrepancies of various types. Plans and procedures should reflect the administration's strategies, objectives, critical success factors, risks, and tactics where possible and appropriate, as well as standards and applicable national and international laws. These factors should determine the administration's approach for identifying, analyzing, responding to, and resolving mail discrepancies.

Specifically, a postal administration must plan for how it will

- identify mail discrepancy events (e.g., through a problem reporting activity or through monitoring)
- analyze the events and determine an appropriate response (e.g., opening an investigation, physically isolating mail, returning mail to the sender)
- prioritize events, in case decisions must be made about which events to respond to, due to limited resources
- respond to events (e.g., a local response or a coordinated national postal administration response)
- close events
- structure and staff the plan (by assigning individuals or groups to specific roles or by creating a specialized response team or similar group)

A postal administration should develop and document its plans and procedures for handling mail discrepancies in accordance with UPU standards and outline the specific objectives of

the plan for each type of mail discrepancy. The objectives of the plan should be translated into specific actions and assigned to individuals or groups to be performed when a discrepancy occurs.

Typical Work Products

1. Mail discrepancy plans and procedures
2. Updates to mail discrepancy plans and procedures

Subpractices

1. Define and document mail discrepancy plans and procedures.
2. Review plans and procedures with relevant stakeholders and get their commitment.
3. Revise mail discrepancy plans and procedures as necessary.

   Refer to CERT-RMM IMC:SG5, Establish Incident Learning, for guidance on performing post-discrepancy reviews, capturing lessons learned from handling mail discrepancies, and using these to inform revisions to mail discrepancy plans and procedures.

IMT:SG5.SP2 Identify and Address International Mail Discrepancies During Transportation

Discrepancies during the transportation of international mail are identified and addressed in accordance with plans and procedures.

A postal administration must be able to identify mail discrepancy events as they occur, as well as determine when an event or a series of events constitutes an incident that requires further handling and escalation (e.g., a coordinated and planned response, such as an investigation). Identifying events in a timely manner may help to contain their operational impact and the cost of addressing them.

Some incidents, such as mail damaged or lost during transportation and mail delayed beyond service agreements, will be reported to the origin IMPC or postal administration by the destination IMPC or postal administration, mailers, and other external individuals and entities.

Occurrences of non-compliance with mail transportation standards in the following categories are identified and addressed as mail discrepancies:

- nonmailable matter, including certain dangerous and hazardous goods
- receptacle, despatch, and consignment identifying information, including duplication
- dimensions and weight
- packaging and containers
- forms, bills, tags, barcodes, and other required documentation
- EDI and other forms of exchanging mail scan and status information
- signatures
- fraudulent mail

- UPU and national laws (Customs and export control, for example)
- mixing of mail categories, classes, or subclasses in receptacles and despatches

Examples of access, availability, sanctity, custody, and visibility discrepancies are

- failure to achieve end-to-end service standards and agreements
- failure to execute chain-of-custody rules
- theft of mail
- loss of mail including a despatch missing from a despatch series
- suspicious mail
- delay of mail (such as flight delays)
- damage to mail, including damage caused by weather (for example, wet mail), malfunctions of transportation equipment, and malfunctions of mail sorting and screening equipment
- broken seals (containers, receptacles, open postal items)
- mail opened and examined by unauthorized personnel
- invalid, missing, and rejected scans
- failure of mail sorting, scanning, and screening technologies
- misrouted or missent mail (for example, a receptacle arrives at the wrong destination IMPC)
- bad or illegible barcodes and labels

Postal items that are not marked in accordance with visibility standards and whose postage does not sufficiently reflect the category, class, subclass, supplementary services and attributes of the postal item to which they are affixed are identified and addressed as mail discrepancies.

Typical Work Products

1. Discrepancy events identified during the processing of outbound mail
2. Discrepancy events identified during the transportation of outbound mail
3. Discrepancy events identified during the transportation of inbound mail
4. Discrepancy events identified during the processing of inbound mail
5. Discrepancy events identified during the execution of mail resilience controls

Subpractices

1. Detect and report mail transportation discrepancy events (as described in CERT-RMM IMC:SG2, Detect Events).

   Such events are identified during outbound processing, outbound transportation, inbound transportation, and inbound processing of mail and in the execution of mail access, availability, sanctity, custody, and visibility controls. For example, a destination IMPC submits a Bulletin of Verification (BV) or a Verification Note (VN) to the origin

IMPC if postal items arrive wet, damaged, tampered with, or a despatch is missing in a despatch series.

2. Address mail transportation discrepancy events according to mail discrepancy plans.

International Mail Transportation Process Area References

[1] UPU Postal Security Group: http://www.upu.int/en/activities/postal-security/about-postal-security.html

[2] *UPU Postal Transport Guide*, February 2014. Received from Greg Crabb, April 2014. The October 2013 version is available here: http://www.upu.int/en/activities/transport/publications.html

[3] *Catalogue of UPU Standards*, 30 October 2013. http://www.upu.int/en/activities/standards/standards-documents.html

[4] *UPU Letter Post Manual*, December 2013. http://www.upu.int/en/activities/letter-post/letter-post-manual.html

[5] *UPU Parcel Post Manual*, December 2013. http://www.upu.int/en/activities/parcels/parcel-post-manual.html

[6] *UPU S58 Postal security standards – General security measures*, July 2013. http://www.upu.int/en/activities/postal-security/security-standards.html

[7] *UPU S59 Postal security standards – Office of exchange and international airmail security*, July 2013. http://www.upu.int/en/activities/postal-security/security-standards.html

[8] *UPU Standards Glossary*, July 2013. http://www.upu.int/en/activities/standards/standards-documents.html

[9] *UPU Transport Service Agreement template*. http://www.upu.int/en/activities/transport/about-transport.html

[10] *General information on UPU standards*, 30 October 2013. http://www.upu.int/en/activities/standards/standards-documents.html

[11] *Future of Mail by Air Standard Operating and Messaging Draft 1.4*, International Post Corporation. http://www.ipc.be/en/Operational-services/Streamlining_processes/Fomba

[12] “EDI: Providing end-to-end airmail visibility” (brochure), UPU, International Air Transport Association, and International Post Corporation. vhttp://www.upu.int/en/activities/transport/upu-iata-cooperation.html

[13] Universal Postal Union. “M39: CARDIT/RESDIT – Data flow version V2,” UPU International Bureau, Berne, Switzerland.

References

[Allen 2014a] Allen, Julia H.; Crabb, Gregory; Curtis, Pamela D.; Mehravari, Nader; White, David W. *CERT Resilience Management Model Mail-Specific Process Areas: Mail Induction, Version 1.0* (CMU/SEI-2014-TN-010). Software Engineering Institute, Carnegie Mellon University, August 2014. http://www.sei.cmu.edu/library/asset-view.cfm?assetID=296355

[Allen 2014b] Allen, Julia; Crabb, Gregory; Curtis, Pamela, D.; Mehravari, Nader; & White, David W. *CERT Resilience Management Model Mail-Specific Process Areas: Mail Revenue Assurance, Version 1.0* (CMU/SEI-2014-TN-011). Software Engineering Institute, Carnegie Mellon University, August 2014. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=296378

[Caralli 2011] Caralli, Richard A.; Allen, Julia H.; White, David W. *CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience*. Addison-Wesley, 2011. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=30375

[Crabb 2012] Crabb, G. U.S. "Postal Inspection Service Use of the CERT Resilience Management Model" (CERT podcast). Software Engineering Institute, Carnegie Mellon University, August 2012. http://www.cert.org/podcasts/podcast_episode.cfm?episodeid=6e2258d2-de92-c7df-d7d2b43bebcef8a0&pageid=34576

[Crabb 2014] Crabb, G.; Allen, Julia H.; Mehravari, Nader; & Curtis, Pamela D. *Improving the Security and Resilience of U.S. Postal Service Mail Products and Services Using the CERT® Resilience Management Model* (CMU/SEI-2013-TN-034). Software Engineering Institute, Carnegie Mellon University, January 2014. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=77277

[Joch 2013] Joch, A. "Operational Resilience: Bringing Order to a World of Uncertainty." *Federal Computer Week*, July 8, 2013. http://fcw.com/articles/2013/07/08/exectech-operational-resilience.aspx

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	August 2014	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
CERT Resilience Management Model—Mail-Specific Process Areas: International Mail Transportation (Version 1.0)	FA8721-05-C-0003

6. AUTHOR(S)

Julia H. Allen, Gregory Crabb, Pamela D. Curtis, Sam Lin, Nader Mehravari, & Dawn Wilkes

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2014-TN-012

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

Developing and implementing measurable methodologies for improving the security and resilience of a national postal sector directly contribute to protecting public and postal personnel, assets, and revenues. Such methodologies also contribute to the security and resilience of the mode of transport used to carry mail and the protection of the global mail supply chain. Since 2011, the U.S. Postal Inspection Service (USPIS) has collaborated with the CERT® Division at Carnegie Mellon University's Software Engineering Institute to improve the resilience of selected U.S. Postal Service (USPS) products and services. The CERT Resilience Management Model (CERT-RMM) and its companion diagnostic methods served as the foundational tool for this collaboration.

This report includes one result of the USPIS/CERT collaboration. It is an extension of CERT-RMM to include a new mail-specific process area for the transportation of international mail. The purpose is to ensure that all international mail is transported in accordance with the standards established by the Universal Postal Union (UPU), which is the governing body that regulates the transportation of international mail.

16. PRICE CODE	15. NUMBER OF PAGES
CERT-RMM, USPS, USPIS, resilience, mail specific, international mail transportation, Universal Postal Union, UPU	53

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL