

**Doc 9985  
AN/492  
RESTRICTED**



# **Air Traffic Management Security Manual**

---

Approved by the Secretary General  
and published under his authority

First Edition — 2013

International Civil Aviation Organization

**AVA** Documents  
Document Sharing Hub



Doc 9985  
AN/492  
RESTRICTED



# Air Traffic Management Security Manual

---

Approved by the Secretary General  
and published under his authority

First Edition — 2013

International Civil Aviation Organization

Published in separate English, Arabic, Chinese, French, Russian  
and Spanish editions by the  
INTERNATIONAL CIVIL AVIATION ORGANIZATION  
999 University Street, Montréal, Quebec, Canada H3C 5H7

For ordering information and for a complete listing of sales agents  
and booksellers, please go to the ICAO website at [www.icao.int](http://www.icao.int)

*First Edition*

**Doc 9985, Air Traffic Management Security Manual**

Order Number: 9985

ISBN 978-92-9249-289-2

© ICAO 2013

All rights reserved. No part of this publication may be reproduced, stored in a  
retrieval system or transmitted in any form or by any means, without prior  
permission in writing from the International Civil Aviation Organization.

## AMENDMENTS

Amendments are announced in the supplements to the *Catalogue of ICAO Publications*; the Catalogue and its supplements are available on the ICAO website at [www.icao.int](http://www.icao.int). The space below is provided to keep a record of such amendments.

## RECORD OF AMENDMENTS AND CORRIGENDA

[illegible][illegible]



## FOREWORD

Standards and Recommended Practices (SARPs) related to maintaining the security of civil aviation operations were first adopted by the International Civil Aviation Organization (ICAO) Council on 22 March 1974 and published as Annex 17 — *Security — Safeguarding International Civil Aviation against Acts of Unlawful Interference* to the *Convention on International Aviation*. The provisions of this Annex require, inter alia, States to establish and implement a National Civil Aviation Security Programme (NCASP).

The applicability of the NCASP was initially limited to aircraft operators and airports, focusing primarily on hijacking and bomb threats. However, following the use of aircraft themselves as weapons in the destruction of the New York City (USA) World Trade Centre on September 11, 2001, there has been a heightened awareness of the possibility of other types of security-related events, including the possibility of similar attacks, or attacks against air traffic service facilities and the navigation and surveillance infrastructure.

Therefore, in response to aviation security concerns, the ICAO Council, on 17 November 2010, adopted Amendment 12 to Annex 17. This required States to include ATSPs in the NCASP and to ensure that they implement appropriate security provisions to meet the requirements of the NCASP.

There has also been an increase in the frequency that air traffic service providers (ATSPs) are asked to support various types of national security and law enforcement operations. This support often requires the establishment of temporary airspace/flight restrictions for security-related purposes such as: protecting the movements of Heads of State; conducting airborne surveillance and monitoring operations, often with remotely piloted aircraft (RPAs); restricting access of unvetted aircraft to airspace surrounding major sporting events and other large-scale public gatherings; or provision of information that supports airspace management for security related purposes. ATSPs need guidance concerning provision of services related to security operations. Beyond this, ATSPs also need guidance on protection of air traffic management (ATM) system infrastructure that supports international aviation.

This manual complements the *Aviation Security Manual* (Doc 8973 – Restricted) and provides guidance on security issues specific to ATM in order to assist States and ATSPs in implementing appropriate security provisions to meet the published requirements of the NCASP. In addition, the manual provides guidance to the ATSP on provision of ATM security services in support of national security and law enforcement requirements, and guidance on protection of the ATM system infrastructure from threats and vulnerabilities.



# OVERVIEW

The first decade of the twenty-first century has seen an increase in terrorist activity against a range of targets using a variety of methods. These have ranged from the use of explosive devices in attacks against aircraft, trains, and buildings, to cyber-attacks against information and communications systems. As a result, a number of States have expressed concerns about the possibility that the air traffic management (ATM) system could be subject to attack, and safeguarding the ATM system from security threats has become an issue of increased concern. At the same time, air traffic service providers (ATSPs) have also been more frequently involved in supporting roles in national security and law enforcement situations, including disaster prevention and recovery operations that are not intentionally directed at the aviation system, but could have profound, negative impacts on the aviation system if not managed effectively. These situations often require use of ATM procedures such as temporary airspace/flight restrictions that provide required safety and security measures and minimize the impacts of security events on flight operations in the ATM system.

## 1. THE INTERNATIONAL LEGAL BASIS FOR AVIATION SECURITY

1.1 Because of the international nature of aviation, effective security requires the participation of all States. In order to achieve a uniform application of security provisions, several international legal instruments (conventions) have been developed. They provide the basis for the uniform implementation of security provisions worldwide.

1.2 The following conventions deal specifically with unlawful interference with aircraft:

- a) The Convention on Offences and Certain Other Acts Committed On Board Aircraft (the Tokyo Convention), signed in Tokyo on 14 September 1963.
- b) The Convention for the Suppression of Unlawful Seizure of Aircraft (The Hague Convention), signed in The Hague on 14 October 1971.
- c) The Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (the Montreal Convention), signed in Montreal on 23 September 1971.
- d) The Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 23 September 1971, done at Montreal on 24 February 1988.
- e) The Convention on the Marking of Plastic Explosives for the Purpose of Detection, done at Montreal on March 1991.
- f) The Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (the Beijing Convention), signed in Beijing on 10 September 2010.
- g) The Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft (the Beijing Protocol), signed in Beijing on 10 September 2010.

These conventions cover a wide range of types of unlawful interference with aircraft, air navigation facilities, and airports.

1.3 In the present context, the most important aspect of the provisions contained in these conventions is that they place an obligation on the States party to them to enact legislation to make the acts defined in the conventions offences punishable by severe penalties under the laws of those States.

## 2. STATE RESPONSIBILITIES FOR AVIATION SECURITY

### *Legislation*

2.1 The first step for a State in establishing aviation security is the enactment of the legislation necessary to give effect to these conventions. Since Standards and Recommended Practices (SARPs) relating to aviation security first became applicable in 1975, this legislation should generally be in place already. However, when implementing ATM security for the first time, States should check that the relevant legislation adequately covers acts of unlawful interference with air traffic service facilities, and provision of ATM security services required by the National Civil Aviation Security Programme (NCASP).

2.2 While the creation of offences and the imposition of penalties for acts of unlawful interference with aviation are important, it is also important to put measures in place to ensure that, to the extent practicable, the entire aviation system is protected against security threats. No security system can guarantee that the protective measures will be able to prevent all attacks, so it is necessary that security planning includes the development and implementation of procedures for responding to incidents involving unlawful interference.

### *National Civil Aviation Security Programme (NCASP)*

2.3 Annex 17 requires States to develop and implement an NCASP, which should specify the roles and responsibilities of all the organizations and agencies, including ATSPs that may be involved in security operations. The NCASP addresses the whole range of security activities including, inter alia, threat and risk assessment, staff selection and training (in security-related matters), access control and other preventive security measures, management of acts of unlawful interference, and quality control.

2.4 Not all provisions of the NCASP will be applicable to the ATSP. The NCASP identifies the specific responsibilities of each of the parties that have a role in security operations.

2.5 ICAO has developed a model NCASP to act as a guide for the States. The model NCASP is published in Doc 8973 – Restricted.

2.6 To ensure the effectiveness of the NCASP, each State must enact legislation establishing an appropriate authority for aviation security. This authority will then be responsible for developing the NCASP and amending it when necessary. It must also enact legislation requiring those parties with responsibilities under the NCASP to implement appropriate security provisions to meet the requirements of the NCASP.

### *The National Civil Aviation Security Committee*

2.7 Because the maintenance of security across the whole aviation system involves a large number of different agencies and organizations, Annex 17 requires States to establish a National Civil Aviation Security Committee. The role of this committee is to facilitate coordination of security activities among these different agencies and organizations. The membership of this committee comprises representatives of all parties with a role under the NCASP. Depending on how services are structured in a particular State, this may include (in addition to the appropriate authority for aviation security) members from the following groups:

- a) ATSPs;
- b) aircraft operators;
- c) airport operators;
- d) customs authorities;
- e) Immigration authorities;
- f) intelligence organizations;
- g) law enforcement authorities (LEA);
- h) military; and
- i) providers of contracted security services.

#### *Airport Security Committee*

2.8 In addition to the National Civil Aviation Security Committee, Annex 17 requires the establishment of an airport security committee for each civil airport. The local air traffic services (ATS) unit should be represented on this committee.

#### *International coordination*

2.9 Although aviation security remains a national responsibility, the increased possibility of international threats makes it necessary to maintain a high level of cooperation among States. The appropriate authority for civil aviation security should establish coordination procedures with corresponding authorities in adjacent States, and agreements should be established concerning the exchange of security information. ATS units should already have established Letters of Agreement (LOAs) with adjacent ATS units within one State or in other States, detailing the communications and coordination procedures. If these LOAs do not already address procedures related to security, they should be updated as part of the planning for implementation of ATM security procedures.

2.10 This collaborative, cooperative approach is necessary to ensure that ATM security management policies and provisions will be able to successfully counter a whole range of acts of unlawful interference, terrorism, or other events which threaten persons or facilities or could result in the disruption of the ATM system's ability to provide services.

### **3. DISTINCTIONS BETWEEN AVIATION SECURITY AND ATM SECURITY**

3.1 This manual provides guidance on ATM Security with the objective of assisting States and ATSPs in (1) implementing aviation security SARPs, (2) protecting ATM system infrastructure, and (3) executing additional security related functions.

*Aviation security definition*

3.2 Doc 8973 – Restricted states that the primary objective of aviation security is “ensuring the protection and safety of passengers, crew, ground personnel, the general public, aircraft, and airport facilities”.<sup>1</sup>

*Aviation Security Standards and Recommended Practices (SARPs)*

3.3 The Ninth Edition of the ICAO Annex 17 (Security – 2011) recognizes the important role ATSPs have in aviation security by introducing the following two SARPs in the Amendment 12:

*“3.5 Air traffic service providers. Each Contracting State shall require air traffic service providers operating in that State to establish and implement appropriate security provisions to meet the requirements of the national civil aviation security programme of that State.”*

*“4.9 Measures relating to cyber threats. Recommendation.— Each Contracting State should develop measures in order to protect information and communication technology systems used for civil aviation purposes from interference that may jeopardize the safety of civil aviation.”*

3.4 All SARPs in Annex 17 are applicable to international operation. Additionally, States are required to ensure that measures designed to safeguard against acts of unlawful interference are applied to domestic operations, to the extent practicable, based on a security risk assessment carried out by the relevant national authorities.

3.5 ATSPs contribute to aviation security in the prevention of, and response to, acts of unlawful interference. This contribution to aviation security usually involves ATSP airspace management for ATM security purposes. Specific ATSP responsibilities for airspace management for ATM security purposes should be identified in agreements with air defence and law enforcement agencies to ensure proper integration of responsibilities of all agencies directly responsible for the State's airspace security. Secure airspace is one of the layers of defence along with the ground-based security of aircraft, people, baggage, cargo/mail, and the airport and other aviation related infrastructure.

3.6 Aviation security is supported by ATM security in its concerns with safeguarding civil aviation against acts of unlawful interference. Acts of unlawful interference are acts or attempted acts such as to jeopardize the safety of civil aviation and include, but are not limited to:

- a) unlawful seizure of aircraft in flight or on the ground;
- b) destruction of an aircraft in service;
- c) hostage-taking on board aircraft or on aerodromes;
- d) forcible intrusion on board an aircraft, at an airport or on the premises of an aeronautical facility;
- e) introduction on board an aircraft, or at an airport of a weapon, hazardous device, or material intended for criminal purposes;
- f) use of an aircraft in service for the purpose of causing death, serious bodily injury, or serious damage to property or environment; and

---

1. Aviation Security Manual (Doc 8973 – Restricted)

- g) communication of false information that jeopardizes the safety of an aircraft in flight or on the ground, passengers, crew, ground personnel, or the general public at an airport or on the premises of a civil aviation facility.

#### *ATM security definition*

3.7 ATM security concerns a broader range of issues than just aviation security. ATM Security is defined in ICAO Circular 330, Civil/Military Cooperation in Air Traffic Management, as:

*“The contribution of the ATM system to civil aviation security, national security and defence, and law enforcement; and the safeguarding of the ATM system from security threats and vulnerabilities.”*

#### *The dual requirements of ATM security*

3.8 ATM security differs from aviation security in the sense that ATM security has dual requirements of protection of the ATM system against threats and vulnerabilities and the provision of ATM security services in support of organizations and authorities engaged in aviation security, national security, defence, and law enforcement. Thus, the ATM security role has a traditional internal role of protection of the ATM system itself and an operational role in the support of certain aspects of aviation security as well as national security and law enforcement.

## **4. THE SCOPE OF ATM SECURITY**

4.1 In order to set the context within which ATM security provisions operate, this section provides an ATM security operational concept, and then concludes with a summary of the ATM security scope.

#### *ATM operational concept for security*

4.2 The security role of ATM is recognized as an essential component of the future ATM system in the *Global Air Traffic Management Operational Concept* (Doc 9854). This document outlines a role for ATM security beyond aviation security to meet national security requirements, assist in protecting against intentional and unintentional threats, and provide continuity of service during security threats and unusual circumstances. It also emphasizes the contribution by the ATM provider to ATM security, and for the protection of the ATM system against this broader range of threats.

#### *National security*

4.3 The ATM system should meet national security requirements outlined in the following statement of the ICAO vision for the integrated, harmonized, and globally interoperable ATM system:

*“To achieve an interoperable global air traffic management system, for all users during all phases of flight, that meets agreed levels of safety, provides for optimum economic operations, is environmentally sustainable and meets national security requirements.”*

#### *Threat protection and security service*

4.4 Doc 9854 defines security as protection against both intentional (e.g., unlawful interference) and unintentional threats. It also emphasizes the need for the ATM provider to contribute to security, and for the protection of ATM system against this broader range of threats.

*“Security refers to the protection against threats that stem from intentional acts (e.g., terrorism) or unintentional acts (e.g., human error, natural disaster) affecting aircraft, people or installations on the ground. Adequate security is a major expectation of the ATM community. The ATM system should therefore contribute to security, and the ATM system, as well as ATM-related information, should be protected against security threats.”*

#### *Continuity of ATM service*

4.5 Doc 9854 lists continuity of service as one of the guiding principles for the on-going development of the ATM system. The protection of the ATM system infrastructure is required to ensure, to a reasonable degree, the continuity of this critical service against a variety of threats. It states the following:

*“The realization of this concept [continuity of service] requires contingency measures to provide maximum continuity of service in the face of major outages, natural disasters, civil unrest, security threats or other unusual circumstances.”*

#### *Other security services*

4.6 Doc 9854 lists other essential entities that the ATM system will provide information to or may receive information from. These include, within the security domain, the entities set out below:

- a) Air defence systems and military control systems will need timely and accurate information on flights and ATM system intents. They will be involved in airspace reservations, notification of air activities and in enforcing measures related to security.
- b) Search and rescue organizations will need timely and accurate information on aircraft in distress and accidents. Such information plays an important role in the quality of the search function.
- c) Aviation accident/incident investigation authorities will need to examine recordings of flight trajectory data and ATM actions.
- d) Law enforcement (including customs and police authorities) will need flight identification and flight trajectory data, as well as information about traffic at aerodromes.
- e) Regulatory authorities will need to implement the regulatory framework within the legal powers given to them and to monitor the safety status of the ATM system.

#### *ATM Security Scope — the Summary*

4.7 ATM security includes security services captured in aviation security SARPs and the broader expectation outlined in Doc 9854. ATM security includes:

- a) the safeguarding of the ATM system from security threats and vulnerabilities (ATM protection); and
- b) the provision of security services that contribute to civil aviation security, national security, defence, and law enforcement (ATM security operations).

4.8 ATM protection refers to internal security services provided and consumed by the ATSP. Some examples of internal security services by the ATSP:

- a) cyber-security services to protect cyber systems; and
- b) physical protection of facilities.

4.9 ATM security operations for external security services provided by the ATSP but consumed by State agencies, partners, and stakeholders. Some examples of external security services are:

- a) support for air defence interdiction;
- b) search and rescue efforts;
- c) aiding law enforcement response (e.g., border protection);
- d) air traffic control (ATC) during unlawful interference to aircraft in flight;
- e) VIP movements; and
- f) support for emergency response to natural disasters.

#### *Organization of the Manual*

4.10 In line with the dual nature of ATM security as described above, the remaining part of this manual consists of the following:

- a) glossary: acronyms and definitions;
  - b) Part A: Protection of ATM System Infrastructure;
  - c) Part B: ATM Security Operations; and
  - d) appendices.
-



# TABLE OF CONTENTS

|                                                                                                                  | <i>Page</i>  |
|------------------------------------------------------------------------------------------------------------------|--------------|
| Glossary .....                                                                                                   | (xix)        |
| Explanation of terms.....                                                                                        | (xxi)        |
| <br><b>PART I — ATM SYSTEM INFRASTRUCTURE PROTECTION</b>                                                         |              |
| <b>Chapter 1. Introduction .....</b>                                                                             | <b>I-1-1</b> |
| 1.1 Background .....                                                                                             | I-1-1        |
| 1.2 Principles for ATM system infrastructure protection .....                                                    | I-1-1        |
| <b>Chapter 2. Governance and organization.....</b>                                                               | <b>I-2-1</b> |
| 2.1 Programme objectives.....                                                                                    | I-2-1        |
| 2.2 State responsibilities.....                                                                                  | I-2-1        |
| 2.3 Regulatory drivers .....                                                                                     | I-2-2        |
| 2.4 Policy.....                                                                                                  | I-2-2        |
| 2.5 Structure, authority and responsibility.....                                                                 | I-2-5        |
| <b>Chapter 3. Facility physical security.....</b>                                                                | <b>I-3-1</b> |
| 3.1 Introduction.....                                                                                            | I-3-1        |
| 3.2 Facility physical security and access control .....                                                          | I-3-1        |
| 3.3 Facility layers of defence and mitigation options .....                                                      | I-3-3        |
| <b>Chapter 4. Personnel security.....</b>                                                                        | <b>I-4-1</b> |
| 4.1 Introduction.....                                                                                            | I-4-1        |
| 4.2 Aviation security requirements .....                                                                         | I-4-1        |
| 4.3 Personnel security programme.....                                                                            | I-4-2        |
| <b>Chapter 5. Information and communication technology (ICT) system security (including cybersecurity) .....</b> | <b>I-5-1</b> |
| 5.1 Introduction.....                                                                                            | I-5-1        |
| 5.2 Background .....                                                                                             | I-5-1        |
| 5.3 Information and communication technology (ICT) security controls .....                                       | I-5-2        |
| 5.4 Next-Generation ATM system considerations .....                                                              | I-5-6        |
| <b>Chapter 6. Contingency planning for ATM security .....</b>                                                    | <b>I-6-1</b> |
| 6.1 Introduction.....                                                                                            | I-6-1        |
| 6.2 Roles and responsibilities between States and ATSPs .....                                                    | I-6-1        |
| 6.3 Air traffic service backup plans for ATM security.....                                                       | I-6-2        |
| 6.4 Contingency planning framework for ATM security .....                                                        | I-6-4        |

**PART II — ATM SECURITY OPERATIONS**

|                                                                                               |               |
|-----------------------------------------------------------------------------------------------|---------------|
| <b>Chapter 1. Introduction .....</b>                                                          | <b>II-1-1</b> |
| 1.1 Background .....                                                                          | II-1-1        |
| 1.2 Interagency collaboration .....                                                           | II-1-1        |
| 1.3 Special planning considerations .....                                                     | II-1-2        |
| <b>Chapter 2. ATM contribution to safeguarding against unlawful interference .....</b>        | <b>II-2-1</b> |
| 2.1 The security role of the ATSP in relation to other Organizations .....                    | II-2-1        |
| 2.2 ATM security functions for aviation security .....                                        | II-2-2        |
| 2.3 Strategic operations security functions .....                                             | II-2-3        |
| 2.4 Tactical operations security functions .....                                              | II-2-4        |
| <b>Chapter 3. ATM support for law enforcement .....</b>                                       | <b>II-3-1</b> |
| 3.1 Overview .....                                                                            | II-3-1        |
| 3.2 Laser threats .....                                                                       | II-3-1        |
| 3.3 Man-portable air defence system (MANPADS) threats .....                                   | II-3-2        |
| <b>Chapter 4. Disasters and public health emergencies .....</b>                               | <b>II-4-1</b> |
| 4.1 ATM support for disaster response and recovery .....                                      | II-4-1        |
| 4.2 Communicable disease and other public health risks on board aircraft .....                | II-4-2        |
| <b>Chapter 5. Airspace management for ATM security .....</b>                                  | <b>II-5-1</b> |
| 5.1 Monitoring and reporting over security identification zones .....                         | II-5-1        |
| 5.2 Emergency security control of air traffic .....                                           | II-5-2        |
| 5.3 Creation, promulgation and monitoring of temporary airspace/flight restrictions .....     | II-5-3        |
| <b>Chapter 6. Organizing for effective ATM security operations .....</b>                      | <b>II-6-1</b> |
| 6.1 Overview .....                                                                            | II-6-1        |
| 6.2 Strategic security planning and operations .....                                          | II-6-2        |
| 6.3 Tactical security operations .....                                                        | II-6-5        |
| 6.4 Special interoperations security for civil, military and law enforcement operations ..... | II-6-6        |
| 6.5 ATM security operations administration .....                                              | II-6-7        |

**APPENDICES**

|                                                                  |                |
|------------------------------------------------------------------|----------------|
| <b>Appendix A. Security risk management process .....</b>        | <b>App A-1</b> |
| 1. Introduction .....                                            | App A-1        |
| 2. Security risk management process .....                        | App A-1        |
| 3. Security risk management — organizational collaboration ..... | App A-7        |
| <b>Appendix B. Cybersecurity in ICT security .....</b>           | <b>App B-1</b> |
| 1. Introduction .....                                            | App B-1        |
| 2. Concepts and definitions .....                                | App B-1        |
| 3. Cyber ICT security requirements .....                         | App B-3        |
| 4. Security measures for critical cyber ICT infrastructure ..... | App B-5        |

|                                                                                                | Page           |
|------------------------------------------------------------------------------------------------|----------------|
| <b>Appendix C. ICT security controls .....</b>                                                 | <b>App C-1</b> |
| 1. Introduction.....                                                                           | App C-1        |
| 2. Control categories .....                                                                    | App C-1        |
| 3. Level of controls .....                                                                     | App C-3        |
| <b>Appendix D. National and regional examples of provision for ATM security services .....</b> | <b>App D-1</b> |
| 1. In-flight security incident management framework in Europe .....                            | App D-1        |
| 2. In-flight security event procedures in the United Kingdom.....                              | App D-7        |
| 3. United States domestic events network procedures.....                                       | App D-13       |

---



# GLOSSARY

## ACRONYMS

|         |                                                                          |
|---------|--------------------------------------------------------------------------|
| ADS-B   | Automatic dependent surveillance — broadcast                             |
| ADS-C   | Automatic dependent surveillance — contract                              |
| ATC     | Air traffic control                                                      |
| ATIS    | Automatic terminal information service                                   |
| ATM     | Air traffic management                                                   |
| ATS     | Air traffic services                                                     |
| ATSP    | Air traffic service providers                                            |
| CAA     | Civil aviation authority                                                 |
| CBRN    | Chemical, biological, radiological and nuclear                           |
| CNS     | Communications, navigation, and surveillance                             |
| COMLOSS | Loss of radio communications                                             |
| CPDLC   | Controller-pilot data link communications                                |
| ETA     | Estimated time of arrival                                                |
| EU      | European Union                                                           |
| FIR     | Flight information region                                                |
| FL      | Flight level                                                             |
| HVAC    | Heating, ventilation and air-conditioning                                |
| ICAO    | International Civil Aviation Organization                                |
| ICT     | Information and communication technology                                 |
| IDENT   | Identification feature in the identification, friend or foe (IFF) system |
| IED     | Improvised explosive device                                              |
| IFF     | Identification, friend or foe                                            |
| IFSO    | In-flight security officer                                               |
| IT      | Information technology                                                   |
| LEA     | Law enforcement authority                                                |
| LOA     | Letter of Agreement                                                      |
| MANPADS | Man-portable air defence system(s)                                       |
| MOA     | Memorandum of Agreement                                                  |
| MOU     | Memorandum of Understanding                                              |
| NAVAID  | Navigational aid                                                         |
| NCASP   | National civil aviation security programme                               |
| NEXTGEN | Next-generation air transportation system                                |
| NGA     | National governmental authority                                          |
| NOTAM   | Notice to Airmen                                                         |
| NSA     | National supervisory authority                                           |
| PANS    | Procedures for air navigation services                                   |
| QRA     | Quick Reaction Alert                                                     |
| RPA     | Remotely piloted aircraft                                                |
| RPG     | Rocket-propelled grenades                                                |
| RTF     | Radio transmission facility                                              |
| SARP    | Standards and recommended practices                                      |
| SESAR   | Single European sky ATM research                                         |
| SOP     | Standard operating procedure                                             |
| SRM     | Safety risk management                                                   |

|      |                                    |
|------|------------------------------------|
| SSR  | Secondary surveillance radar       |
| SWIM | System-wide information management |
| TOI  | Track of interest                  |
| UAS  | Unmanned aircraft system(s)        |
| VFR  | Visual flight rules                |
| VHF  | Very high frequency                |
| VIP  | Very important person              |
| VOR  | VHF omnidirectional radio range    |
| WHO  | World Health Organization          |

---

## EXPLANATION OF TERMS

**Acts of unlawful interference.** Acts or attempted acts such as to jeopardize the safety of civil aviation and air transport:

- a) unlawful seizure of aircraft;
- b) destruction of an aircraft in service;
- c) hostage-taking on board aircraft or on aerodromes;
- d) forcible intrusion on board an aircraft, at an airport or on the premises of an aeronautical facility;
- e) introduction on board an aircraft or at an airport of a weapon or hazardous device or material intended for criminal purposes;
- f) use of aircraft in service for the purpose of causing death, serious bodily injury, or serious damage to property or environment; and
- g) communication of false information such as to jeopardize the safety of an aircraft in flight or on the ground, or passengers, crew, ground personnel or the general public, at an airport or on the premises of a civil aviation facility.

**Air Domain.** The global airspace; all manned and unmanned aircraft operating in the global airspace; all people and cargo present in the global airspace; and all aviation-related infrastructure.

**Airspace management for ATM security.** Management of airspace to:

- a) deter, prevent, detect and resolve where possible airborne threats including those associated with unlawful interference;
- b) provide for emergency security control of air traffic; and
- c) initiate and monitor temporary airspace/flight restrictions in support of national security and law enforcement activities.

**Air traffic management (ATM).** The dynamic, integrated management of air traffic and airspace including air traffic services, airspace management and air traffic flow management — safety, economically and efficiently — through the provision of facilities and seamless services in collaboration with all parties and involving airborne and ground-based facilities.

**Air traffic management security.** The safeguarding of the ATM system from security threats and vulnerabilities; and the contribution of the ATM system to civil aviation security, national security and defence, and law enforcement.

**Air traffic management system.** A system that provides ATM through the collaborative integration of humans, information, technology, facilities and services, supported by air and ground- and/or spaced-based communications, navigation and surveillance.

**Air traffic service provider (ATSP).** Annex 17 uses the term ATSP in the Amendment 12 Standard for aviation security. Therefore, this manual uses the term ATSP to be consistent with the ICAO Standard. However, States that must use the term air navigation service provider (ANSP) by law should substitute ANSP for ATSP. ANSP should be considered synonymous with ATSP as used in this manual.

**ATM system infrastructure.** ATM system infrastructure includes people, procedures, information, resources, facilities, including control centres, airports and equipment, including communications, navigation and surveillance (CNS) and information systems.

**ATM system infrastructure protection.** The protection of the ATM system infrastructure through information and communication technology (ICT) security, physical security and personnel security.

**Aviation security.** The safeguarding of civil aviation against acts of unlawful interference. This objective is achieved by a combination of measures and human and material resources.

**ICT security.** The application of security measures to protect information and data processed, stored or transmitted in ICT systems (analog and digital) against loss of integrity, confidentiality and availability, whether accidental or intentional, and to prevent loss of integrity or availability of the systems themselves. ICT security measures include measures for protection of computers and networks (cyber systems), information and data transmission, emission and cryptographic security. ICT security measures also include detection, documentation and countering of threats to information and communications and to the ICT systems.

*Integrity* means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity.

*Confidentiality* means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

*Availability* means ensuring timely and reliable access to and use of information.

**Information and communication technology (ICT).** ICT is an umbrella term that includes any information or communication device (analog or digital) or application, encompassing: radio, television, telephones smartphones, smartpads, computer and network hardware and software, data storage systems and devices, satellite systems, surveillance systems, navigation systems, as well as the various services and applications associated with them.

**Personnel security.** The part of security concerned with procedures designed to assess whether an individual can, taking into account his loyalty, trustworthiness and reliability, be authorized to have initial and continued access to classified information and controlled areas without constituting an unacceptable risk to security.

**Physical security.** The part of security concerned with physical measures designed to safeguard people; to prevent unauthorized access to equipment, facilities, material and documents; and to safeguard them against a security incident.

**Risk.** Potential for an unwanted outcome resulting from an incident, event or occurrence. Risk can be estimated by considering the likelihood of threats, vulnerabilities and consequences or impacts.

**Risk assessment.** Continual, on-going exercise to update the complete range, magnitude and type of credible threats and their likelihood, based on reliable information from the intelligence services, the vulnerabilities to them, and the possible consequences or impacts of loss of degradation from successful attacks.

**Temporary airspace/flight restrictions.** Temporary airspace/flight restrictions are ATM procedures established via Notice to Airmen (NOTAMS) which provide geographically-limited, short-term, restrictions to specific flight activity for national security, law enforcement, or safety reasons. Temporary airspace/flight restrictions specify ATM procedures for temporary security identification zones that enhance security, safety and flexible use of airspace required for activities such as national events, major sporting events, air shows, crisis management for natural disasters, space launches, and movements of national leaders. Temporary airspace/flight restrictions are not the same as ICAO restricted areas. Temporary airspace/flight restrictions are conditions of flight imposed as a result of application of rules of the air or air traffic services practices or procedures and do not constitute calling for designation as a restricted area.

**Threat.** For aviation security, threats are deliberate, intentional acts carried out by individuals or organizations, generally with a hostile purpose. However, national security and law enforcement can be impacted by intentional and unintentional threats. Natural disasters and unintentional spread of pandemic disease would be classified as unintentional threats. The likelihood or probability for intentional threats is a function of the means or capability to act, the motivation to do so and the intention to do so. The likelihood or probability of unintentional threats depends on human factors, weather factors and location of ATM system infrastructure. Human factors could lead to human error and loss of critical ATM services. Location and weather determine potential for impacts on the ATM system infrastructure from flood, fire, earthquakes, hurricanes, tornados, temperature extremes, solar effects and accidents on nearby transport systems or production and storage facilities for chemical, biological, radiological and nuclear (CBRN) material that could result in facility evacuation, etc.

**Track of interest (TOI).** A TOI is displayed data representing an airborne object that poses a threat or potential threat to security. Indicators for a potential TOI may include, but are not limited to:

- a) non-compliance with ATC instructions or aviation regulations;
- b) prolonged loss of communications;
- c) unusual transmissions or unusual flight behaviour;
- d) unauthorized intrusion into controlled airspace or a security identification zone;
- e) non-compliance with published temporary airspace/flight restrictions or other issued flight restriction/security procedures; and
- f) unlawful interference with airborne flight crews, up to and including hijacking.

In certain circumstances, an airborne object may become a TOI based on specific and credible intelligence pertaining to that particular aircraft/object, its passengers or its cargo.

**Track of interest (TOI) resolution.** A TOI will normally be considered resolved when:

- a) the aircraft/object is no longer airborne;
- b) the aircraft complies with ATC instructions, aviation regulations and/or issued flight restrictions/security procedures, including temporary airspace/flight restrictions;
- c) radio contact is re-established and authorized control of the aircraft is verified;
- d) the aircraft is intercepted and intent is verified to be non-threatening/non-hostile;

- e) TOI was identified based on specific and credible intelligence that was later determined to be invalid or unreliable; and
- f) displayed data is identified and characterized as invalid.

**Vulnerability.** Physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or attack or susceptible to a given hazard. Vulnerability increases the risk of unwanted outcome from an incident, event or occurrence.

---

**PART I**

**ATM SYSTEM INFRASTRUCTURE PROTECTION**



# Chapter 1

## INTRODUCTION

### 1.1 BACKGROUND

1.1.1 As described in the overview of air traffic management (ATM) security, the definition of ATM security includes the protection of the ATM system against threats, and the support that the ATM system provides to organizations and authorities engaged in aviation security, national security, defence, and law enforcement.

1.1.2 Part A of the manual addresses the protection of the ATM system infrastructure. Part B of the manual addresses the provision of ATM security services to support various organizational security requirements.

1.1.3 ATM system infrastructure includes people, procedures, information, resources, facilities, and equipment. Facilities include control centres and airports. Equipment includes communications, navigation and surveillance (CNS), and information systems.

1.1.4 ATM system infrastructure protection refers to the protection of the ATM system infrastructure through information and communication technology security, physical security, and personnel security. It also includes the provisions for continuity of service during an emergency or disasters.

1.1.5 Therefore, an ATM security programme for infrastructure protection should have the following components:

- a) physical security;
- b) personnel security;
- c) information and communication technology (ICT) security; and
- d) security contingency planning to address security issues for disaster recovery and continuity of operation.

### 1.2 PRINCIPLES FOR ATM SYSTEM INFRASTRUCTURE PROTECTION

#### 1.2.1 Security programme for mission support

The security programme allows the air traffic service provider's (ATSP) organization to accomplish its operational missions and has become a necessity for the ATSP to counter threats and reduce vulnerabilities. While strengthening security measures, it is important to remember that security is not an end by itself. A security programme enables the ATSP to execute its missions in a manner consistent with stakeholder expectations. The security programme protects the ATSP from service degradations by ensuring the integrity, confidentiality and availability of the organization's operational functions. However, the security practice should not impede the execution of the ATSP's missions or that of its delivery partners. In evaluating security control alternatives, the ATSP must weigh the security benefits against the impacts on the efficiency and effectiveness of operational functions.

### 1.2.2 Risk-based security management

Managing risk is a key element of the ATSP organization's security programmes. While the concept of zero risk might be appealing, it is impossible to design a risk-free security programme. ATSP organizations can maximize the investment value of a security programme by establishing a strategy and objectives that attain an optimal balance between operational goals and related risks, and deploying resources efficiently and effectively. Based on acceptable risk levels, the ATSP should evaluate and select risk mitigation alternatives to manage risks.

### 1.2.3 Integrated security management

1.2.3.1 Managing the ATSP's security risks is a complex and multifaceted undertaking that requires a holistic approach. It should be fully integrated into every aspect of the organization. ATM security should be analysed in terms of the key elements of the ATM system, including people, procedures, ICT systems and other technical equipment and facilities with associated supporting infrastructures. While security measures for these components require different specialists, overall security management decisions must be considered from an organizational level first. These elements are not independent, but are interrelated in their contributions to the delivery of services.

1.2.3.2 The ATSP is as secure as its weakest link. For example, poorly trained air traffic controllers can subvert the protection of a well-designed ICT system. On the other hand, the security measures for one ATSP component may be leveraged by other elements (e.g., physical access control serving as a layer of security for the critical information assets inside the facility). The holistic approach allows an understanding of the various relationships, thereby promoting a comprehensive, consistent and efficient approach.

### 1.2.4 Consider the full spectrum of security measures

1.2.4.1 In developing security measures, the ATSP organization needs to think broadly. Security measures are not limited to technology; they also include policy and process. In addition, security measures can be applied at different phases of a security incident such as reducing the likelihood of successful attack or lessening the impact of the attack.

1.2.4.2 Early security measures have focused on protective measures to reduce the likelihood of successful attacks. With ever increasing threats and the vulnerability of open systems, there is a need for security measures that mitigate the consequences of adverse and potentially catastrophic events. The best strategy for developing security measures is to seek a defence in depth, with specific controls aimed at reducing the risk by one or more of the following:

- a) improved ability to detect an attack;
- b) reducing the vulnerability to attack;
- c) developing contingency measures to reduce of the impact of the loss of any elements of the ATM service; and
- d) shortening the recovery time to reduce the impact of an attack.

## Chapter 2

### GOVERNANCE AND ORGANIZATION

#### 2.1 PROGRAMME OBJECTIVES

2.1.1 The objectives of the ATSP's security programme for ATM system infrastructure protection are:

- a) to support aviation security and the primary goal to ensure the protection and safety of passengers, crew, ground personnel, the general public, aircraft and facilities of an airport serving civil aviation, in all matters related to safeguarding against acts of unlawful interference perpetrated on the ground or in flight; and
- b) to support the execution of the ATSP's missions and minimize the disruption of the ATM service from intentional and unintentional threats.

2.1.2 To meet these objectives, a comprehensive organizational structure needs to be established with clearly defined organizational security policy, roles, responsibilities and methods of implementation. Before developing the security policy, the ATSP should understand the regulatory requirements from national authorities and consider the separation of the oversight entity from the implementation entity.

#### 2.2 STATE RESPONSIBILITIES

##### 2.2.1 State regulations

2.2.1.1 States should promulgate appropriate legislation or regulations that provide penalties for any person wilfully trespassing or attempting to trespass into a designated security-restricted area of the airport, including ATSP facilities. Such legislation or regulations should also apply to trespassing or attempted trespass at off-airport communications, surveillance and navigation aid (NAVAID) sites.

2.2.1.2 States should also include appropriate provisions for the protection of critical ATM information and communication technology systems against cyberthreats and interferences in their National Civil Aviation Security Programmes (NCASPs) and other relevant national programmes.

##### 2.2.2 State oversight

2.2.2.1 In addition to requiring ATSPs to implement a security programme, States have an oversight responsibility in relation to ATM Security. Although aviation security oversight is defined as a function by means of which States ensure the effective implementation of the security-related Standards and Recommended Practices (SARPs) and associated procedures contained in the Annexes to the Chicago Convention (primarily in Annex 17, but including the security-related provisions of Annex 9) and related International Civil Aviation Organization (ICAO) documents, aviation security requirements should also be accompanied by security procedures appropriate for all aspects of air traffic management.

2.2.2.2 The nature of the relationship between the State regulatory body and the ATSP will depend upon the structure of the aviation services within the State. In some States, the appropriate authority for aviation security will be within the Civil Aviation Authority (CAA); in other States it may be a separate government agency. In some States, the CAA will also be the ATSP, while in other States the ATSP will be a separate organization. Regardless of the situation the body responsible for security oversight should be separate from the provider.

2.2.2.3 However, if the CAA is responsible for both service provision and oversight, there should be a functional separation between the two. One approach for achieving this separation is to have the oversight entity report directly to the CAA chief executive, rather than reporting through the operational management structure.

## 2.3 REGULATORY DRIVERS

2.3.1 The ATSP security programme for infrastructure protection should be governed by multiple national regulations for aviation security, ICT security, and critical infrastructure protection. When developing the security programme, the ATSP should integrate all applicable requirements. In support of aviation security, the ATSP organization<sup>1</sup> should participate in:

- a) the National Civil Aviation Security Committee;
- b) the Airport Security Committee; and
- c) the planning, training, and exercise for responding to unlawful interference/seizure of aircraft.

2.3.2 As noted earlier, the NCASP specifies the security responsibilities of all relevant stakeholders in aviation security, including the ATSP, and is the expression of a State's aviation security policies. Policies relevant to the ATSP are affected through the development and implementation of an ATM security programme. For example, the NCASP Model in the *Aviation Security Manual* (Doc 8973 – Restricted), contains a section on the protection of air navigation facilities. These requirements should be incorporated into the ATSP's security programme. Moreover, as a key component of aviation transportation and as the owner/operator of ICT systems, the ATSP is subject to additional national regulations such as those for infrastructure and ICT security. Therefore, the NCASP should also incorporate these regulatory requirements by requiring the ATSP to implement security controls for critical ATM ICT systems.

## 2.4 POLICY

2.4.1 Security policy is the first step for an ATSP committed to enhancing its security performance. The ATSP's security policy sets the tone and context for the ATSP's security provisions. It captures the security views of senior management and the overall intention and direction of the organization.

2.4.2 A security policy is both functional and informative. From the functional perspective, it guides the ATSP organization in its current and future actions. From the information perspective, it communicates the ATSP's commitment to security to stakeholders and the public.

---

1. The ATSP organization supporting aviation security should also include those responsible for operations security and those responsible for the security programme for ATM system infrastructure protection.

2.4.3 To ensure that the security policy is integrated and balanced with other policies, the ATSP's security policy should be formulated by considering the following major factors:

- a) the ATSP mission;
- b) the ATSP vision;
- c) core values;
- d) stakeholder requirements; and
- e) guiding principles.

2.4.4 The ATSP mission is an expression of the reason it exists and the function it serves in society. The vision is the organization's aspirations and often serves its motivational purpose. Core values are the cultural and ethical positions that the organization adopts. Stakeholder requirements are expectations for the ATM organization by internal and external stakeholders; these stakeholders may include the military, aircraft operators, regulators, suppliers, operations partners, employees, and the public. The guiding principles focus or define the parameters of the actions.

2.4.5 Several key features are essential for any effective and credible security policy. These features are discussed in the paragraphs that follow.

#### 2.4.5.1 *Clear and specific guidance for risk management*

2.4.5.1.1 The security policy needs to be relevant to the service and activities of the ATM organization as it sets the management direction and parameters for risk management. The following areas must be defined:

- a) strategic security goals for the ATM organization;
- b) risk tolerability (acceptable or tolerable levels of risk); and
- c) risk assessment triggers.

2.4.5.1.2 *Strategic security goals.* Strategic security goals define objectives, legal and regulatory requirements, and service obligations to third parties. These goals guide the next activity of the security management framework. They ensure that the scope and evaluation of the threat impacts on the critical infrastructure assets are pertinent and consistent with the strategic goals. Therefore, goals need to be sufficiently specific to relate to groups of infrastructure assets and security incident types. For example, a security goal for information assets may include a classification system that identifies types of information, related impacts, and specific minimum requirements on operational procedures or protection technology.

2.4.5.1.3 *Risk tolerability.* An important responsibility for ATSP management is deciding on a tolerable level of risk. The risk tolerability may take the form of a fixed policy or a framework for management decisions (e.g., what level of risk requires a signatory). The framework approach offers the advantage of dealing with the potentially dynamic nature of risk tolerability. The policy on risk appetite must include the acceptable level for both risks and impacts. Impact-based policy allows for consideration of risks that are unlikely, but have very high impact. It is often addressed through the development of the operations continuity plan.

2.4.5.1.4 *Risk assessment triggers.* The security policy should specify when risk assessment is required. It is conducted periodically to ensure that the security provisions are continually adapted to the evolving threat environment. In addition, it is prudent and desirable to reassess risk in response to:

- a) security incidents that take into account new knowledge concerning vulnerabilities or threats;
- b) security policies that may alter risk priorities or risk appetite;
- c) threat environments that exhibit a new type of attack or a new attacker strategy; and
- d) system changes that are triggered by the configuration control processes or during the development of a new system.  
(See Appendix A, Risk Management)

#### 2.4.5.2 *Explicit description of governance and accountability*

2.4.5.2.1 The ATSP's security policy should describe the governance structure. This includes a description of the person responsible for setting policy and overseeing the execution, and the person responsible for protecting specific assets. It also may require additional supporting policies. Finally, the security policy should include a commitment statement from all levels of the organization. Senior management and staff should commit to the following goals:

- a) achieving secure work performance;
- b) protecting the organization's assets and services;
- c) continually improving the security management process; and
- d) complying with all current applicable requirements.

2.4.5.2.2 While security is the collective responsibility of everyone within the organization, the ultimate accountability rests with the senior management. Thus, the security policy must highlight accountability at the senior level of management.

#### 2.4.5.3 *Internal consistency*

The security policy should be consistent with other ATM policies (e.g., safety, quality, environment, human resources). The policy should be appropriate for threats faced by the organization and for the scale of the organization's operations.

#### 2.4.5.4 *External consistency*

The security policy should define the scope of the organization's security management and its relationships with external parties such as other ATM organizations, military, airports, etc. Interfaces with these external parties need to be agreed with the National Supervisory Authority (NSA), ensuring overall coherence on a national scale and in the aviation sector.

#### 2.4.5.5 *Broad and timely circulation*

The security policy should be documented, implemented, and maintained. It also should be communicated to all employees and relevant third parties, including contractors and visitors. When appropriate, the security policy should be available to all stakeholders. When the policy is changed, it should be announced and made available to all parties in a timely fashion.

## 2.5 STRUCTURE, AUTHORITY AND RESPONSIBILITY

2.5.1 The ATM organization should integrate security in the management process by establishing a formal structure that clearly defines roles, responsibilities, and line of authority to achieve the goals of the security management policy, objectives, targets, and programmes.

2.5.2 The management structure should be clear, documented, communicated and effectively implemented. Interfaces between the line management and the security management functions should be identified. Personnel should be evaluated regularly to monitor their effectiveness in implementing the policy.

2.5.3 Managing the ATSP's security risks requires the involvement of the entire organization. It entails the senior management's commitment to provide the strategic vision, top-level goals, and objectives; mid-level leaders to plan and manage projects; and individuals on the front line to develop, implement, and operate the systems that support the organization's core missions and operations processes.

2.5.4 Senior management should ensure that the ATSP maintains a security programme for ATM system infrastructure protection. They should demonstrate their commitment to the development and implementation of the security provisions by:

- a) appointing a senior manager with security responsibilities (senior security manager);
- b) ensuring the availability of adequate resources; and
- c) managing stakeholder expectations.

2.5.5 The senior security manager should be the top security executive in the ATSP organization. This person should be responsible for providing oversight and coordination of security efforts across the ATSP organization ensuring that resources needed are available and used effectively. The ATSP security programme should include plans for facility physical security; personnel security; and information, communication, and technology system security. With the increasing reliance on information technology (IT) and the ever increasing complexity of IT, the ATSP may find it beneficial to appoint another senior security manager who will focus on cyber ICT security. This person would be responsible for cybersecurity pertaining to information and communication technology and for introducing appropriate cyber technology solutions to other security programmes.

2.5.6 Each aspect of the security programme will be explained in the chapters that follow.

---



## **Chapter 3**

# **FACILITY PHYSICAL SECURITY**

### **3.1 INTRODUCTION**

3.1.1 The facility physical security programme provides a safe environment for ATSP employees, assets, contractors, and visitors. Because the ATSP serves a critical function in civil aviation, physical security also prevents assets from being compromised and used to jeopardize the safety and security of passengers, crews, and the public.

3.1.2 Physical security describes measures that are designed to deny access to unauthorized personnel from physically accessing a building, resource, or stored information. Physical security can be a simple locked door or a complex layered approach using measures for deterrence, detection and defence. Security measures should be deployed in a manner that ensures effective use of the available resources. In other words, security measures need to be cost-effective for the anticipated threats and appropriate for assets' criticality rankings. See Appendix A for more information.

3.1.3 The following section describes physical security requirements specified in Doc 8973 – Restricted followed by a more comprehensive but general description of physical security programmes that the ATSP may follow.

### **3.2 FACILITY PHYSICAL SECURITY AND ACCESS CONTROL**

#### **3.2.1 Airports and ATSP facilities**

3.2.1.1 This section is based on Doc 8973 – Restricted, Section 11.2 and associated appendices, which address the protection requirements for the ATSP's facilities from the perspective of their being part of an airport facility or a vulnerability of an airport facility. Physical security measures should be supported by properly trained personnel, and sound and comprehensive contingency planning.

3.2.1.2 The Aviation Security Manual recommends that States promulgate appropriate legislation or regulations that provide penalties for anyone wilfully trespassing or attempting to trespass into a designated security-restricted area of the airport facility, including the ATSP's facilities. Such legislation or regulations should also apply to trespassing or attempts to trespass at off-airport communications and NAVAID sites.

#### **3.2.2 ATM facilities (ACCs, approach control facilities, air traffic control towers)**

3.2.2.1 Security measures are required to protect essential ATM facilities against intentional and unintentional acts. Loss of ATM facilities could have severe implications on the safety and security of civil aviation operations. Before designing appropriate security protection and measures for ATM facilities, the ATSP should make a comprehensive risk assessment for each ATM facility.

3.2.2.2 This risk assessment would require vulnerability assessments for each facility, as well as an impact analysis of the consequences of a light, medium or severe disruption of service. Then, the scope of possible attacks or

disaster effects should be listed for each ATM facility, as well as the potential impact of such attacks on the safety and security of the public, passengers, and staff, on the operations of the airport, and on the entire Flight Information Region (FIR) where the facility is located. Note that attacks or disasters affecting ATM facilities through disruption of major NAVAIDS, water supply, power supply, etc. could cause major disruptions of service, making use of an airport or an entire FIR impractical until repairs are done (e.g., restoring major NAVAIDS, water supply, power supply), and the facility re-establish critical ATM services.

3.2.2.3 The ATSP should develop a multi-layered approach for protecting ATM facilities based upon a security risk assessment and cost-effectiveness analysis. Such measures would help ensure that an attack against the first layer would not automatically stop operations. In addition, it would provide time for taking additional protective measures for other layers until impacts are mitigated on the first layer. (Layers of defence are described in more detail in the next section.) If a multi-layer approach is impossible or too costly, the ATSP still needs to maintain protection measures that meet safety and security and operational objectives.

### 3.2.3 ATM facility design considerations

ATM Facilities could be attacked from the exterior using conventional weapons such as rocket-propelled grenades (RPG) or small arms fire; or they could also be attacked internally by an intrusion. Disruption of the power supply could also have negative consequences for the operations of the facility. Consideration should be given to addressing these three major threats at the design stage to make sure that potential perpetrators could not launch an RPG or fire high-calibre or long-range small arms from a hidden location near the facility, or that potential perpetrators could not gain access to the facility easily from public areas without a timely reaction from the security forces based at the airport (may include the ATSP's security staff, law enforcement or military forces). Ideally, ATM facilities should be surrounded by open areas such as parking or access roads) with adequate video surveillance. In addition, auxiliary generators should be installed to protect the power supply in all areas. Specific considerations for shape, layout, materials and technical rules should be followed in order to strengthen structures, minimize impacts, and safeguard resilience.

### 3.2.4 Navigation aids (NAVAIDs)

3.2.4.1 NAVAIDs could be located within the perimeter of the airport, close to the airport, or in remote locations. When NAVAIDs are located inside the airport perimeter, all protective equipment and measures installed for protecting the perimeter are a first line of defence. It is important to ensure that all NAVAIDs grouped in the same area inside the airport perimeter have additional protective devices and measures such as anti-intrusion systems and video surveillance.

3.2.4.2 For NAVAIDs located close to the airport but outside the perimeter, additional protective devices and measures are necessary to detect potential attacks immediately. The perimeter of the airport could be adjusted to embrace all NAVAIDs located close to the airport if possible. Alternatively, the installation of an intrusion detection system is recommended.

3.2.4.3 For remote NAVAIDs, video surveillance with automatic recording of the last 12 hours of the facility's exterior is recommended. Warning capabilities should be installed so that a proper reaction to the loss of a remote site can be initiated. If NAVAIDs cannot be adequately protected by physical security measures and intrusion detection systems, they should be visited frequently by security staff or maintenance technicians. Staffed installations should have strict access control measures, and admission to such installations should include the requirement to produce a valid identification permit.

### 3.2.5 ATM system components

Ideally, the facilities hosting ATM system components should have their security systems closely coordinated with the appropriate local and national authorities for aviation security, based upon a security risk assessment. Threat and vulnerability assessments should be performed so that risks are known and appropriate countermeasures are developed and implemented to reduce the risks. In many States, ATM system components are privatized and/or located away from the airport vicinity; therefore, special attention should be placed on protective measures for such facilities.

## 3.3 FACILITY LAYERS OF DEFENCE AND MITIGATION OPTIONS

3.3.1 This section intends to provide the ATSP with a broad spectrum of mitigation measures by offering a list of mitigation measures as well as a description of the layers of defence for facility protection.

### 3.3.2 Facility components

A facility is composed of multiple components. When developing the security programme, the ATSP must consider the facility by its components to ensure a comprehensive basis for identifying potential vulnerabilities, assessing consequence of damage or loss, and determining mitigation options. These components are generally as follows:

- a) site;
- b) architectural design;
- c) structure systems;
- d) utility systems;
- e) mechanical systems;
- f) plumbing and gas systems;
- g) electrical systems;
- h) fire alarm systems; and
- i) ICT systems.

### 3.3.3 Layers of defence

The layers of defence extend from the critical assets outward by identifying perimeter layers and determining security strategies.

- *First layer of defence.* The first layer of defence requires an understanding of the surrounding area. It focuses on buildings, installations, and infrastructure outside the site perimeter. This includes a careful study of surrounding streets, access points for utilities (e.g., electricity, water, sewer, gas, other fuels), access points for ICT, and any other nearby infrastructure that could have an impact on facility operations such as chemical plants and rail lines, roads, and waterways that transport hazardous materials. A release of toxic fumes during manufacture or transport could require evacuation of the facility;
- *Second layer of defence.* The second layer of defence refers to the space that exists between the site perimeter and the assets requiring protection. It involves the design of access points, parking, roadways, pedestrian walkways, natural barriers, security lighting, and signage. For urban areas, it refers specifically to the building yard;
- *Third Layer of Defence.* The third layer of defence refers to protecting the site, controlling the access and minimizing the impact of an attack. It typically involves the hardening of the structures and systems to incorporate effective heating, ventilation, and air conditioning (HVAC) systems and surveillance equipment, and thoughtful design and placement of utilities and mechanical systems.

### 3.3.4 Mitigation options

Figures I-3-1 and I-3-2 provide a spectrum of site mitigation measures for the second and third layers of defence. These measures are listed in ascending order in terms of level of protection, cost, and maintenance effort. While there are many factors affecting the feasibility, cost, and the effectiveness of mitigation measures, this list provides a starting point for the ATSP when considering the design of facility security.



Figure I-3-1. Control options for the second layer of defence

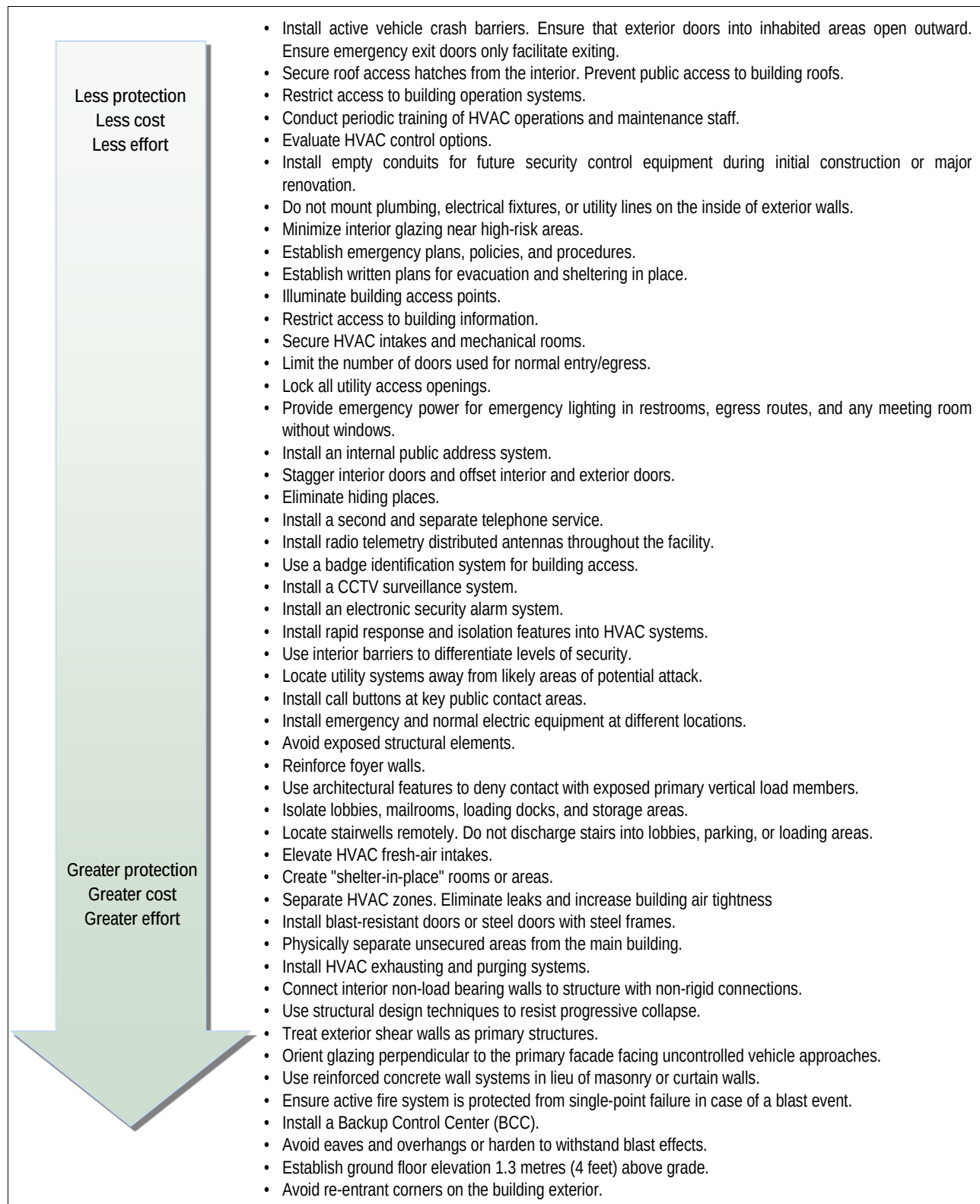


**Figure I-3-2. Control options for the third layer of defence**

## Chapter 4

### PERSONNEL SECURITY

#### 4.1 INTRODUCTION

4.1.1 Personnel security refers to personnel measures for assessing loyalty, trustworthiness and reliability and for granting personnel access to confidential or classified ATM system infrastructure, including information. The ATSP's personnel security programme ensures the integrity of the ATSP's services, including the ability to support aviation security, national security and law enforcement. It also protects the ATSP organization from insider threats resulting from infiltration or employees determined to do harm.

4.1.2 The following section describes personnel security requirements specified in Doc 8973 – Restricted followed by a more comprehensive but general description of personnel security programmes that the ATSP may follow.

#### 4.2 AVIATION SECURITY REQUIREMENTS

4.2.1 Doc 8973 – Restricted, Chapter 8, outlines the personnel selection and training requirements for all entities involved with the national aviation security system. The requirements are provided for security and non-security staff. While the security staff definition in the Aviation Security Manual does not list the security staff for an ATSP, it is assumed that the requirements are applicable to the ATSP security staff that performs similar functions. The ATSP personnel security and security training requirements should be compliant with the State's standards, criteria, and procedures with all national requirements in mind.

4.2.2 The ATSP personnel selection and training process should follow the procedures outlined below to ensure that the employee has sufficient integrity to perform the duties.

##### 4.2.3 Security staff

4.2.3.1 The ATSP's security staff are those persons responsible for implementing security measures such as:

- a) access control;
- b) surveillance and patrolling;
- c) screening of vehicles;
- d) conducting ATM security training;
- e) conducting quality control measures;
- f) personnel security programme; and
- g) ICT security programme.

4.2.3.2 All ATSP security staff or potential employees should undergo background checks and recurrent checks, as needed. Background checks should include searches pertaining to involvement with groups suspected of terrorist or criminal activities or sympathies, and verification of applicants' identities, previous experience and criminal history as legally permissible. Recurrent background checks should occur when employees are required to renew their identification permit cards.

#### **4.2.4 Non-security staff**

4.2.4.1 Non-security staff can be defined as any air traffic control (ATC) provider, technician, or staff member who has duties related to civil aviation operations and could be involved in the implementation of security measures.

4.2.4.2 These non-security staff, especially those requiring access to security restricted areas, should be subject to a background check during the initial selection process and again at regular intervals, in accordance with the provisions of national regulations.

### **4.3 PERSONNEL SECURITY PROGRAMME**

4.3.1 This section provides general guidance for the ATSP personnel security programme. The ATSP may follow this guidance to develop the programme but tailor to their specific situations.

#### **4.3.2 General considerations**

4.3.2.1 The ATSP should establish and maintain a personnel security programme consistent with applicable laws, regulations, and requirements. The personnel security programme should provide a balance between achieving a high level of security and protecting the civil rights and liberties of individuals. The ATSP needs to be compliant with a State's privacy regulations and procedures when collecting, maintaining, using, and disseminating personal information.

4.3.2.2 The ATSP should develop formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls. These controls should include ATSP personnel and contractors. Personnel assigned to sensitive or critical positions will be held to a higher expectation of trust, commensurate with their responsibilities. Personnel security procedures should also be developed for particular ICT systems. Furthermore, the personnel security programme should address the requirements over the lifecycle of an employee (selection and review during employment, transfer, and termination) and should address third-party requirements.

#### **4.3.3 Position risk categorization**

The ATSP should assign a risk (i.e., sensitivity or criticality) designation to all positions and establish screening criteria for individuals filling these positions. The positions' risk designations need to be reviewed and revised, if appropriate, on a periodic basis. This designation needs to be consistent with the State's policy and guidance. The screening criteria should include explicit information on security role appointment requirements (e.g., training, security clearance).

#### **4.3.4 Personnel screening and vetting**

The ATSP should ensure background screening is conducted by proper authorities prior to selecting an individual for a position or authorizing an individual access to the ICT system. The ATSP may accept the eligibility of an individual from

another organization that has conducted a comparable background screening, if it is approved by national laws or regulations. The ATSP should also establish or follow prescribed conditions and frequencies for rescreening. Different rescreening conditions and frequencies may be required for personnel accessing the ICT system, based on the sensitivity of the position and information processed, stored or transmitted by the system. In addition, the ATSP should ensure that all persons together with items carried are subject to screening and security controls prior to entry into facility security restricted areas serving civil aviation operations.

#### **4.3.5 Personnel termination**

4.3.5.1 Upon termination of an individual's employment, the ATSP should: (a) terminate access to restricted facilities and ICT systems; (b) conduct exit interviews; (c) retrieve all security-related organizational property, including ICT systems; and (4) retain access to organizational information and ICT systems formerly controlled by the terminated individual.

4.3.5.2 Exit interviews ensure that individuals understand the security constraints imposed by being a former employee, and that proper accountability is achieved. Examples of security-related property are authentication tokens, system administration technical manuals, keys, identification cards, and building passes.

#### **4.3.6 Personnel transfer**

4.3.6.1 The ATSP should review physical and logical access authorizations to facilities, information, and ICT systems when personnel are reassigned or transferred to other positions within the organization, whether it is temporary or permanent. The ATSP should initiate these organization-defined transfer or reassignment security actions within a specified time, following the formal transfer action.

4.3.6.2 Examples of actions that may be required include: (1) returning old and issuing new keys, identification cards, and building passes; (2) closing previous ICT system accounts and establishing new accounts; (3) changing ICT system access authorizations; and (4) providing for access to official records which the employee had access to at the previous work location and in the previous ICT system accounts.

#### **4.3.7 Access agreements**

The ATSP should identify situations where an access agreement is required, prior to granting access to information and ICT systems. Information requiring special protection measures includes privacy information and proprietary information. Examples of access agreements include nondisclosure agreements, acceptable-use agreements, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with the ICT system to which access is authorized.

#### **4.3.8 Third-party personnel security**

4.3.8.1 The ATSP or Civil Aviation Authority (CAA) should establish personnel security requirements, including security roles and responsibilities for third-party providers (e.g., contractors, suppliers). These requirements should be part of the selection criteria and must be satisfied by third-party providers. The ATSP should also monitor provider compliance.

4.3.8.2 Examples of third-party providers include service bureaus, contractors (including maintenance contractors), and other organizations providing ICT system development, information technology services, outsourced applications, and network and security management.

#### **4.3.9 Personnel sanctions**

The ATSP or CAA should establish and implement a formal sanctions process for personnel failing to comply with established security policies and procedures. The sanctions process should be consistent with applicable State laws, policies, and guidance. This sanctions process is part of the ATSP general personnel policies and procedures, and should be described in access agreements.

#### **4.3.10 Personnel support**

The ATSP or CAA should establish programmes for protecting and supporting employees and other persons with critical knowledge or functions. Examples include security awareness training, identifying and mitigating fear tactics used by terrorist and criminal agents and disaffected insiders, and offering protection and other resources for employees when they are threatened. The ATSP or CAA should also train employees to help detect and counter insider threats by making management aware of suspicious or abnormal behaviour and work practices of other employees.

#### **4.3.11 Visitor control**

The ATSP or CAA should establish and implement visitor control policies for visits by individuals or large groups to each type of ATC facility. Procedures should specify visit registration requirements, ID checks required for entry, escort procedures for hosts during the visit, and restrictions on bringing digital devices, and other types of recording and photographic devices into the facility.

## Chapter 5

# INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) SYSTEM SECURITY (INCLUDING CYBERSECURITY)

### 5.1 INTRODUCTION

5.1.1 Information is an asset to the ATSP organization; it needs to be protected. The ATSP organization may have a great deal of information about employees, passengers, flight crews, flight operations, historical records, and financial status. Should this confidential information fall into the hands of an unauthorized entity, this breach of security could lead to ATM system shutdown, unlawful interference with aircraft flight operations, lawsuits, or loss of life. Protecting confidential information is, therefore, a prime ATM security requirement and, in many cases, an ethical and legal requirement.

5.1.2 ICT security refers to the application of security controls to protect ATM ICT systems against the degradation of integrity, confidentiality and availability from intentional or accidental causes. The ATM ICT system security applies to people, procedures, data, software, and hardware that are used to gather and analyse digital and analogue information used in ATM.

5.1.3 The ATSP should apply a risk management approach in the development of the ICT security programme, similar to the development of other security programmes (See Appendix A, Security risk management process). This chapter provides guidelines that the ATSP can use to select security controls for their ICT system assets and the environment in which they function.

### 5.2 BACKGROUND

5.2.1 Security controls are the safeguards implemented to protect the integrity, confidentiality and availability of ATM ICT systems. Security controls may be management, operational or technical in nature. Controls are used as a synonym for countermeasures or vulnerability mitigation. In summary, integrity, confidentiality and availability are defined below:

- a) integrity is a security objective that ensures information and systems are not modified improperly or accidentally. When integrity is compromised, information may be modified or destroyed;
- b) confidentiality is a security objective that ensures information is not disclosed to unauthorized entities. When confidentiality is compromised, the unauthorized disclosure of information may occur. Confidentiality is often provided by encrypting data that is in transit or stored; and
- c) availability is a security objective that ensures the continuity, reliability, and accessibility of data, resources and services to authorized entities in a timely manner. When availability is compromised, the system may experience a temporary service disruption or a complete loss of service continuity.