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

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

First Edition

Doc 9985, *Air Traffic Management Security Manual*
Order Number: 9985
ISBN 978-92-9249-289-2

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. The space below is provided to keep a record of such amendments.

RECORD OF AMENDMENTS AND CORRIGENDA

AMENDMENTS		
No.	Date	Entered by

CORRIGENDA		
No.	Date	Entered by

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".*[1]

Aviation Security Standards and Recommended Practices (SARPs)

3.3 The Ninth Edition of the ICAO Annex 17 (*Securit*y – 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

Page

PART II — ATM SECURITY OPERATIONS

APPENDICES

Page

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[1] 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.

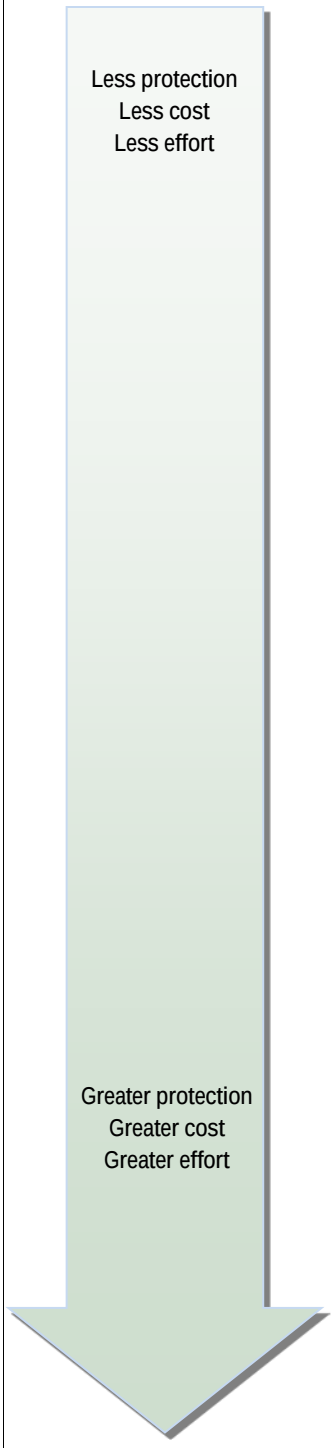
— *First layer of defence.* The first layer of defence requires an understanding of the surrounding area. It focuses on buildings, installations, and infrastructure outside the site perimeter. This includes a careful study of surrounding streets, access points for utilities (e.g., electricity, water, 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.

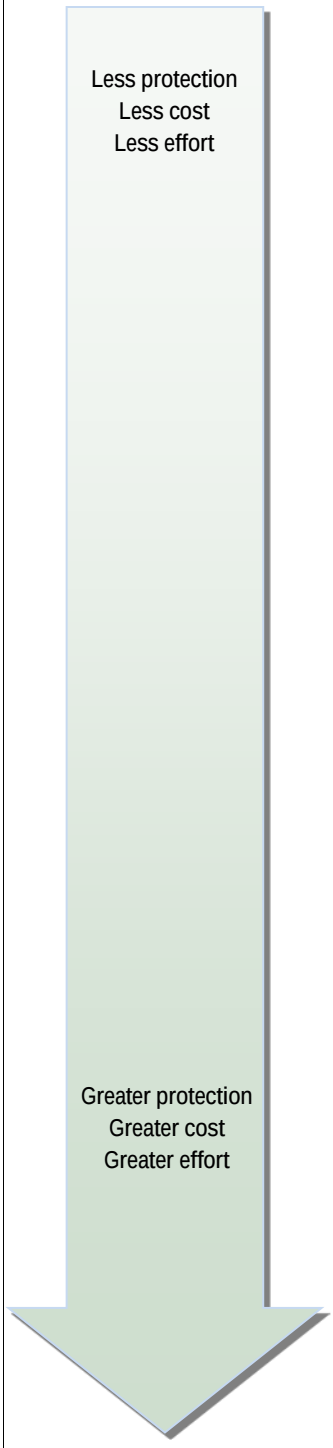
3.3.4 Mitigation options

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.



- Place trash receptacles as far away from the building as possible.
- Remove any dense vegetation that may screen covert activity.
- Use thorn-bearing plant materials to create natural barriers.
- Identify all critical resources in the area (fire and police stations, hospitals, etc.).
- Identify all potentially hazardous facilities in the area (nuclear plants, chemical labs, etc.).
- Use temporary passive barriers to eliminate straight-line vehicular access to high-risk buildings.
- Use vehicles as temporary physical barriers during elevated threat conditions.
- Make proper use of signs for traffic control, building entry control, etc. Minimize signs identifying high-risk areas.
- Introduce traffic calming techniques, including raised crosswalks, speed humps and speed tables, pavement treatments, and traffic circles.
- Identify, secure, and control access to all utility services to the building.
- Limit and control access to all crawl spaces, utility tunnels, and other means of under building access to prevent the planting of explosives.
- Utilize Geographic Information Systems (GIS) to assess adjacent land use.
- Provide open space inside the fence along the perimeter.
- Locate fuel storage tanks at least 30 metres (100 feet) from all buildings.
- Block sight lines through building orientation, landscaping, screening, and landforms.
- Use temporary and procedural measures to restrict parking and increase stand-off.
- Locate and consolidate high-risk land uses in the interior of the site.
- Select and design barriers based on threat levels.
- Maintain as much stand-off distance as possible from potential vehicle bombs.
- Separate redundant utility systems.
- Conduct periodic water testing to detect waterborne contaminants.
- Enclose the perimeter of the site. Create a single controlled entrance for vehicles (entry control point).
- Establish law enforcement or security force presence.
- Install quick connects for portable utility backup systems.
- Install security lighting.
- Install closed circuit television cameras.
- Mount all equipment to resist forces in any direction.
- Include security and protection measures in the calculation of land area requirements.
- Design and construct parking to provide adequate stand-off for vehicle bombs.
- Position buildings to permit occupants and security personnel to monitor the site.
- Do not site the building adjacent to potential threats or hazards.
- Locate critical building components away from the main entrance, vehicle circulation, parking, or maintenance area. Harden as appropriate.
- Provide a site-wide public address system and emergency call boxes at readily identified locations.
- Prohibit parking beneath or within a building.
- Design and construct access points at an angle to oncoming streets.
- Designate entry points for commercial and delivery vehicles away from high-risk areas.
- In urban areas with minimum stand-off, push the perimeter out to the edge of the sidewalk by means of bollards, planters, and other obstacles. In extreme cases, push the line farther outward by restricting or eliminating parking along the curb, eliminating loading zones, or through street closings. For this measure, you need to work with your local officials.
- Provide intrusion detection sensors for all utility services to the building.
- Provide redundant utility systems to support security, life safety, and rescue functions.
- Conceal and/or harden incoming utility systems.

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



- Install active vehicle crash barriers. Ensure that exterior doors into inhabited areas open outward. Ensure emergency exit doors only facilitate exiting.
- Secure roof access hatches from the interior. Prevent public access to building roofs.
- Restrict access to building operation systems.
- Conduct periodic training of HVAC operations and maintenance staff.
- Evaluate HVAC control options.
- Install empty conduits for future security control equipment during initial construction or major renovation.
- Do not mount plumbing, electrical fixtures, or utility lines on the inside of exterior walls.
- Minimize interior glazing near high-risk areas.
- Establish emergency plans, policies, and procedures.
- Establish written plans for evacuation and sheltering in place.
- Illuminate building access points.
- Restrict access to building information.
- Secure HVAC intakes and mechanical rooms.
- Limit the number of doors used for normal entry/egress.
- Lock all utility access openings.
- Provide emergency power for emergency lighting in restrooms, egress routes, and any meeting room without windows.
- Install an internal public address system.
- Stagger interior doors and offset interior and exterior doors.
- Eliminate hiding places.
- Install a second and separate telephone service.
- Install radio telemetry distributed antennas throughout the facility.
- Use a badge identification system for building access.
- Install a CCTV surveillance system.
- Install an electronic security alarm system.
- Install rapid response and isolation features into HVAC systems.
- Use interior barriers to differentiate levels of security.
- Locate utility systems away from likely areas of potential attack.
- Install call buttons at key public contact areas.
- Install emergency and normal electric equipment at different locations.
- Avoid exposed structural elements.
- Reinforce foyer walls.
- Use architectural features to deny contact with exposed primary vertical load members.
- Isolate lobbies, mailrooms, loading docks, and storage areas.
- Locate stairwells remotely. Do not discharge stairs into lobbies, parking, or loading areas.
- Elevate HVAC fresh-air intakes.
- Create "shelter-in-place" rooms or areas.
- Separate HVAC zones. Eliminate leaks and increase building air tightness
- Install blast-resistant doors or steel doors with steel frames.
- Physically separate unsecured areas from the main building.
- Install HVAC exhausting and purging systems.
- Connect interior non-load bearing walls to structure with non-rigid connections.
- Use structural design techniques to resist progressive collapse.
- Treat exterior shear walls as primary structures.
- Orient glazing perpendicular to the primary facade facing uncontrolled vehicle approaches.
- Use reinforced concrete wall systems in lieu of masonry or curtain walls.
- Ensure active fire system is protected from single-point failure in case of a blast event.
- Install a Backup Control Center (BCC).
- Avoid eaves and overhangs or harden to withstand blast effects.
- Establish ground floor elevation 1.3 metres (4 feet) above grade.
- Avoid re-entrant corners on the building exterior.

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 natures. 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 accidently. 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.

5.2.2 To safeguard the ATM ICT system, it is also necessary to address the security of the environment in which these systems function. Therefore, information security is also concerned with physical security, suppliers, infrastructure services, and third parties that ATSP interacts with such as law enforcement, security, and regulatory authorities.

5.3 INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) SECURITY CONTROLS

5.3.1 Development considerations

5.3.1.1 The following guidance was developed by taking into consideration the following two issues:

a) the need to assist organizations in selecting the appropriate controls from the large number specified in the international standards; and

b) the wide range of ATSP organizations and the ICT system types.

5.3.1.2 To address these issues, this guidance includes a catalogue of ICT security controls (refer to Appendix B, Cybersecurity in ICT security). This catalogue is based on the compilation and consolidation of the following international standards:

a) all relevant standards for information communication security in ISO/IEC 27001:2005; and

b) other relevant standards, particularly from COBIT and the ISO/IEC 13335-4 family.

5.3.1.3 The catalogue also incorporates best practices to ensure practical and up-to-date applications of these standards. By following the guidance, the ATSP organization would be compliant with the prevalent international standards.

5.3.1.4 In addition, the ICT security controls can be organized into levels, depending on the risk of ICT systems designated by the organization. The lowest risk requires the lowest level of baseline control; the highest risk requires the highest level of baseline control.

5.3.2 Control categories

5.3.2.1 The ICT security controls can be organized into nine categories:

1. *Organizational direction and policy controls*

   The organizational direction and policy controls deal with the collections of people, external entities, and organizations that adhere to security policies and procedures of a given organization.

   The security policy is a document that is approved by management, distributed to all employees and external entities, covers all systems, and describes the responsibilities of each party relevant to the usages of the systems covered by the policy. It is a living document that undergoes scheduled review cycles and unplanned updates, as needed, to ensure the currency and effectiveness of the policies contained therein. The security policy is also part of the risk management approach for assessing and managing ICT security.

2. *Organization, culture, and management controls*

   The successful development and deployment of a policy-based ICT security system is dependent largely on management participating and supporting the effort with clear and continued commitment to the process.

   The controls provide a mapping of organizational operations objectives to security objectives with well-defined management roles and clear security objectives.

3. *Human resources controls*

   Human resources controls for ICT security relate to employees and contractors, and their roles, responsibilities, and suitability. Risk is examined and reduced by ensuring that they are properly screened and trained for their roles. Of concern are the inherent risks of theft and resource misuse.

4. *Physical and environmental security controls*

   Physical and environmental security controls for ICT security are concerned with ICT security vulnerabilities related to a facility's location, security perimeter, access control techniques, and various security equipment that protects an organization and its ICT assets.

5. *Operation of ICT system controls*

   Operation of ICT system controls ensure that operational security, defined in procedures and policies, is properly implemented. Education of system users helps to ensure that policies are understood and obligations are fulfilled.

6. *Technical mechanisms and infrastructure controls*

   Technical mechanisms and infrastructure controls ensure that appropriate network configuration controls provide sufficient network protection, and that selected technical controls prevent unauthorized entities from accessing system data.

   The principle of least privilege is typically used to ensure that an individual or system is not granted more access than needed to perform their task.

   Examples of controls include firewalls, intrusion detection systems, access control lists, data encryption, passwords, network segregation, and routing control.

7. *Acquisition and development controls*

   Acquisition and development controls for ICT security are ensured through the use of proven system engineering methodologies making sure that security is fully integrated into all the phases of the acquisition and development lifecycle.

8. *Monitoring and audit controls*

   Monitoring and audit controls for ICT security are concerned with security logging of events, audit logs, and fault logs. System alerts and alarm monitors are employed to detect alert conditions and unauthorized system use.

9. *Compliance controls*

Compliance controls for ICT security ensure that systems comply with statutory, regulatory, and contractual agreements and requirements. Controls are typically ensured through system audits.

5.3.2.2 Table I-5-1 below relates the security objectives of integrity, confidentiality and availability to the ICT security controls described above.

5.3.2.3 Cybersecurity is an integral aspect of ICT Security. For more detailed information on cybersecurity refer to the Aviation Security Manual, Chapter 18, on cyber threats to critical aviation information and communication technology systems. See also Appendix B, Cybersecurity in ICT security.

5.3.2.4 The NCASP should highlight three areas of concern for ICT security programmes: 1) the protection of systems against unauthorized access; 2) the prevention of tampering with systems; and 3) detection of attacks on systems. Examples of control categories for accomplishing these objectives are:

a) protect systems against unauthorized access and uses:

1) secure physical perimeter around facility;

2) defend in-depth network security architecture; and

3) identity management and access controls tools;

b) prevent tampering with the systems:

1) file integrity tool; and

2) system segregation of duties and least privileges;

c) detect attacks on the systems:

1) employ intrusion prevention systems;

2) employ intrusion detection systems;

3) security operations monitoring for alerts and alarms; and

4) collection of system logs information.

5.3.2.5 Categorizing the controls by organizational functions allows different functional parts of an organization to relate to a smaller group of controls. However, this does not mean that organizational risk management can focus on a single organizational function to protect a particular asset; usually controls will be needed from several functions.

5.3.3 Risk level of controls

5.3.3.1 ATSP organizations vary in size and types. For example, ATSPs can range from being an organization with a small staff providing a limited range of service (e.g., NAVAIDS) to those managing sophisticated ATC centres. In some States, it is the government agency that provides air traffic services through a wide variety of ATM systems or facilities.

5.3.3.2 To accommodate the range of ATSP organizations and their ICT systems, the appropriate security controls could be grouped into six levels of increasing rigor as illustrated in Appendix C. The key differentiator is the risk level of an ATM ICT system. The risk level varies according to the criticality of the service provided by the ATSP organization, the vulnerability of the ICT system, and the nature of threats.

5.3.3.3 The control levels should be cumulative and correspond to baseline ICT control requirements for ATM organizations. Each control level should have an increasing degree of ICT complexity or ICT assets with increasing risk. For example, Level 1 should be the lowest level and is appropriate for an organization with a limited and isolated ICT system. The highest level would demand a competent implementation of all the control requirements and would be appropriate for the most complex ATSP organizations. The key differentiator is the risk level of an ICT system. The risk level varies according to the criticality of the service provided by the ATSP organization, the vulnerability of the ICT system, and the nature of threats to the ATM system. General characteristics for example control levels are shown in Appendix C along with detailed descriptions of each level for each of the nine organization functions.

Table I-5-1. Control Categories and Integrity, Confidentiality and Availability

ICT Control Category	*Integrity*	*Confidentiality*	*Availability*
Organizational Direction and Policy	Policy ensuring that controls protect data integrity	Organizational policy may dictate the protection of information	Policy ensuring system sized properly to ensure availability
Organization, Culture, and Management	Procedures and policies for handling data	Management procedures and policies for protection of data	Asset identification and maintenance of resources
Human Resources	Employee training	Employee training on handling confidential data	Employee training
Physical and Environmental Security	Security and access controls to data	Secure perimeters and physical protections.	Redundant and backup equipment and sites
Operations of ICT Systems	Change-management control	Procedures to protect removable media; Interconnect policies	Service-level agreements for operations of systems
Technical Mechanisms and Infrastructure	File-integrity tools	Encryption mechanisms	High-availability solutions
Acquisition and Development	Formal change management processes	Operations requirements for data protection	Operations requirements to ensure availability
Monitoring and Audit	Audit logs recording changes	Monitoring and audit performance of the information protection including attacks and attempted attacks.	Monitoring critical system health and usage
Compliance	Adherence to policy concerning loss, destruction, or falsification of data	Cryptographic controls used in compliance with agreements, laws	Compliance with operations continuity plans

5.4 NEXT-GENERATION ATM SYSTEM CONSIDERATIONS

5.4.1 ICT security will play a greater role in the next-generation ATM systems, such as the Next-Generation Air Transportation System (NextGen) in the U.S. and the Single European Sky ATM Research (SESAR) in Europe. As data communication links replace existing voice communication channels, there is a greater need to ensure that data links using security controls are timely and reliable, as they will be vital to the success of the programmes.

5.4.2 System-wide information management (SWIM) provides the opportunity for sharing ATM data such as meteorological, air traffic flow, flight trajectory, and surveillance. The timely, secure, and reliable delivery of the data is paramount in the success of next-generation ATM systems.

Chapter 6

CONTINGENCY PLANNING FOR ATM SECURITY

6.1 INTRODUCTION

6.1.1 Contingency planning should include ATM security considerations and should address the safe and orderly and secure degradation of a service in a contingency situation and its recovery in an orderly manner to the normal capacity operating situation. Continuity of operation ensures that the ATSP organization can securely conduct essential functions for up to a specified period.

6.1.2 First, despite the implementation of preventive and protective controls, security incidents could still happen, and the ATSP needs to prepare for these situations. Second, contingency controls may be viewed as part of the integrated control strategy and offer more cost-effective solutions to protective/preventive controls. Contingency measures allow for the continued operation of mission-essential functions, even when protection fails. This shift of system protection to system resilience represents a major paradigm shift in the security programme.

6.1.3 As discussed in the “Overview”, contingency planning is a regulatory requirement for the ATSP under Annex 11 — *Air Traffic Services*. Because of the similarity of plans for system protection and system resilience, the ATSP may wish to incorporate them into one contingency plan.

6.1.4 This chapter provides a description of ATC backup planning, as required of the ATSP in Annex 11, followed by the description of a general approach to help the ATSP identify and decide the best contingency strategies to meet its ATM security needs.

6.2 ROLES AND RESPONSIBILITIES BETWEEN STATES AND ATSPs

6.2.1 The roles of States stem from Annex 11 to the Chicago Convention, particularly from Section 2.30, Contingency Arrangements, as interpreted by the guidance of Attachment C to Annex 11. States are responsible for providing air traffic services and related supporting services in their airspace. This responsibility extends to the contingency situations for instituting measures to ensure the safety of international civil aviation operations and, where possible, for making provisions for alternative facilities and services. Such measures must include security provisions or there can be no assurance of safety.

6.2.2 As a result, States need to ensure the development of contingency plans by the designated ATSP to whom the services have been delegated. The State can perform the oversight or delegate this task to another entity through proper instruments. States are also responsible for coordinating with other States affected by the contingency plans and, if necessary, concluding State-level agreements.

6.2.3 The ATSP's first responsibility is the development of contingency plans in accordance with State requirements. The preparation phase includes the definition of the controls and the coordination with other stakeholders such as the State (including civil aviation security, military and law enforcement authorities), possibly other ATSPs, and insurance companies. The ATSP is responsible for developing the notification contact list in case an outage occurs and the service is discontinued. The ATSP should also identify the minimal set of information and time for delivery of this information to air traffic service (ATS) units in neighbouring FIRs or States, in coordination with the regulator. The ATSP is also responsible for the implementation of the plan in appropriate cases.

6.3 AIR TRAFFIC SERVICE BACKUP PLANS FOR ATM SECURITY

6.3.1 Damage to facilities and widespread damage to essential infrastructure can severely affect the ability of an ATS unit to continue to provide the normal level of service. If the damage to a facility renders it inoperative, alternative arrangements will be necessary. If the control tower is damaged, limited service may be provided by using portable communications equipment; however, severe damage to an en-route centre would require transferring responsibility for the airspace to another unit.

6.3.2 The ATSP is required, by Section 2.30 of Annex 11, to establish contingency plans for these types of events, as well as other events that could result in disruption of services, such as a fire in an ATC centre.

Note.— Additional information on contingency planning can be found in Attachment C of Annex 11. This addresses situations where changes to the ATS route structure affecting international operations and/or transfer of control of airspace to another State are necessary, requiring a temporary amendment to the Regional Air Navigation Plan.

6.3.3 Plans for delegating air traffic service to another ATSP vary from local backup plans to regional FIRs. The management of these plans is often conducted by a Letter of Agreement (LOA) between adjacent facilities, where circumstances and capabilities for handling non-routine emergencies are identified, developed, and practised through contingency exercises:

a) surveillance coverage;

b) data exchange;

c) communications;

d) airspace and ATSP services;

e) staffing;

f) training;

g) duration; and

h) cost sharing.

6.3.4 Overlapping surveillance coverage at a particular site depends on equipment availability or equipment capability. If overlapping surveillance coverage is not available, ATC procedural separation would be implemented in a non-routine situation, requiring increased separation distances of aircraft. This also will depend on the backup facilities' capability to handle an increased capacity in a particular airspace.

6.3.5 Figure I-6-1 illustrates two options for accomplishing backup coverage in a contingency situation.

6.3.6 In one option, when ATSP B is degraded and it has no other backup options, such as repurposing a simulation or training facility to cover the degradation, ATSP A expands and covers all of ATSP B's area. In the other option, ATSP A and ATSP C expand their coverage and each covers half of ATSP B's area.

6.3.7 During degraded operations, adjacent ATSP facilities may be able to accept backup data exchanged between the degraded facility and the covering facility. Exchanging an air picture and data with an adjacent facility is a common practice in many parts of the world. Consideration could also be given to continuous mirroring of data between adjacent facilities.

6.3.8 Communication links with aircraft in a region may also be exchanged. If they cannot be exchanged, the covering ATSP may use emergency frequency 121.5 MHz and direct aircraft to a frequency with which aircraft might contact the ATSP taking over the airspace duties.

6.3.9 The covering ATSP needs to ensure adequate staffing is available. For the covering staff to handle the additional workload, it is important to have the airspace details of the adjoining sectors, dimensions, and frequencies ready in advance. Consideration could also be given to migrating staff from the failed facility to the covering ATSP facility.

6.3.10 Training for degraded situations should be conducted on a recurring basis (e.g., annually). This will allow for ATSP staff to develop the necessary skill to handle non-routine contingency situations smoothly and provide ATM security services for the affected airspace.

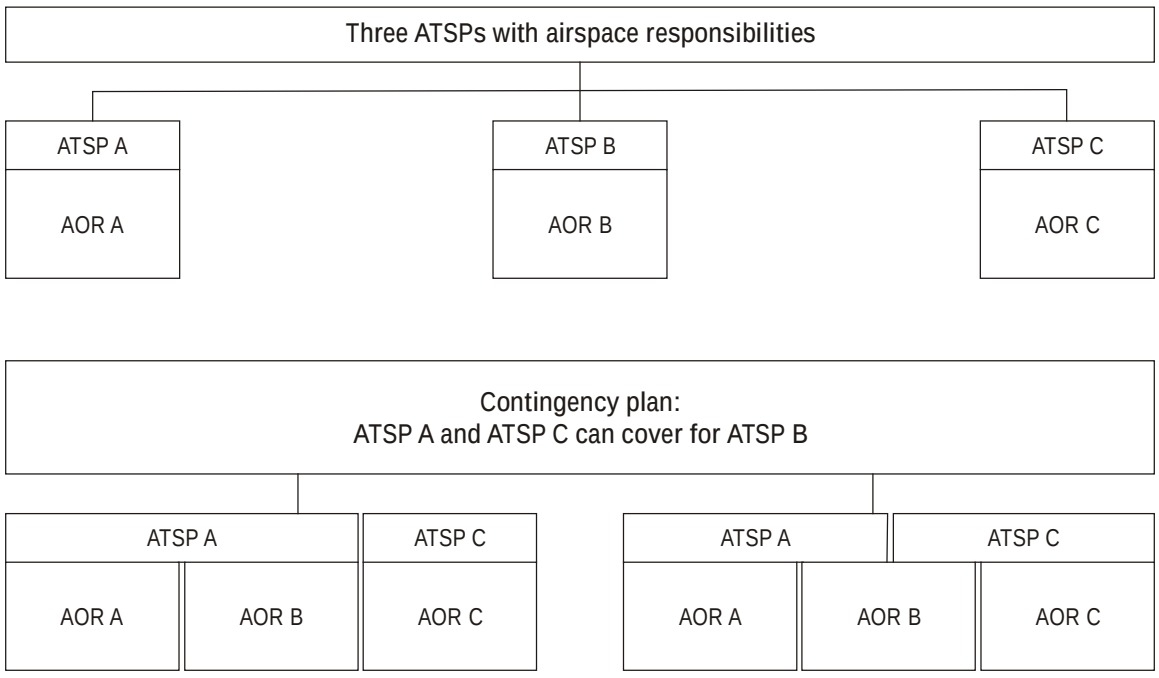


Figure I-6-1. Air traffic service delegation examples

6.3.11 The duration of a degraded operation should be fully considered. If the degraded ATSP has a mobile backup capability or can gain access to one through ICAO assistance, it may require additional time to coordinate; however, it can also ensure that the degraded facilities' staff can continue to operate fully or partially.

6.3.12 Finally, a cost-sharing arrangement should be described in a LOA. Should costs arise, these can be budgeted for and planned.

6.4 CONTINGENCY PLANNING FRAMEWORK FOR ATM SECURITY

6.4.1 This section describes a contingency planning framework which establishes a comprehensive, systematic, and rational approach for ATSP contingency activities, which is illustrated in Figure I-6-2.

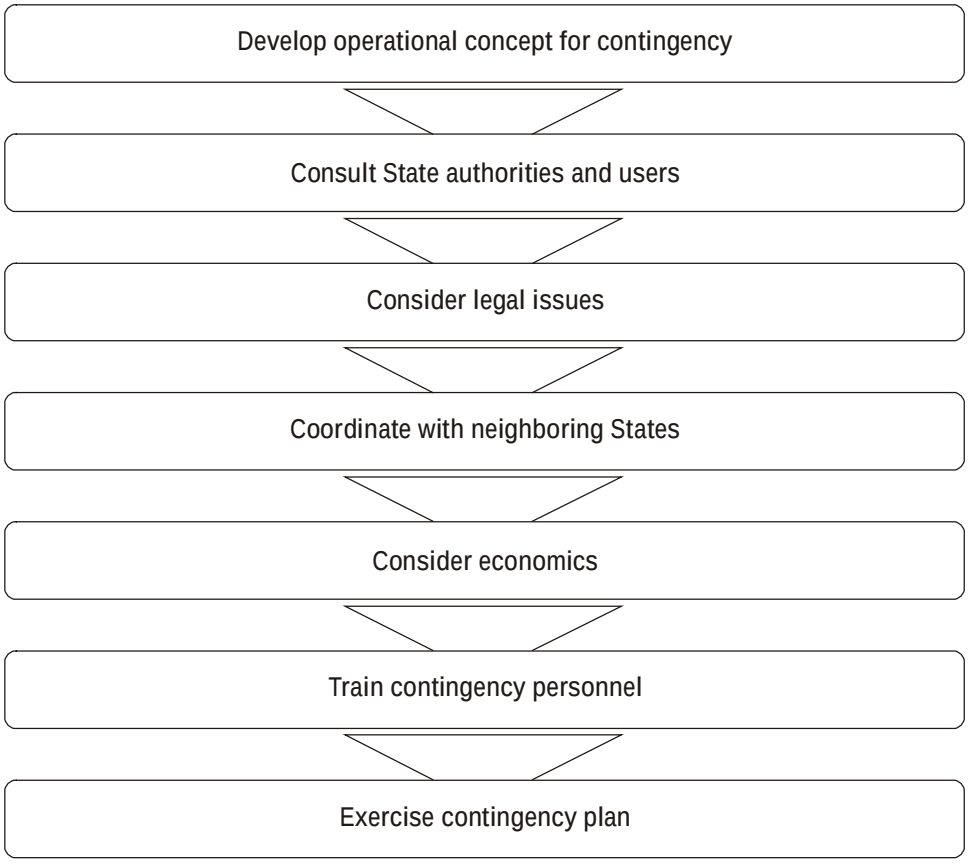


Figure I-6-2. Contingency planning framework

6.4.2 Develop an operational concept for contingency

The operational concept for contingencies considers and documents the following:

a) ATSP contingency policy: It is critical for senior management to clearly define the organization's overall contingency objectives and scope, and to establish the organization's framework and responsibility for contingency planning;

b) Key contingency events and related risks: Develop a list of key contingency events, hazards, and related risk areas that the organization has identified and wishes to protect itself against;

c) Candidate contingency strategies: State the scope, context, and criteria of contingency measures to indicate which contingency strategies are to be further detailed within the contingency plans. For example, when the facility is damaged, contingency measure options may include:

   1) co-located facilities;

   2) multi-use facilities;

   3) centralized facilities; and

   4) sharing international common system solutions with other countries.

6.4.3 Consult State authorities and users

The State authorities (including civil aviation security, military and law enforcement authorities), the ATSPs, and the users (airspace users and airports) should establish a process for developing contingency measure requirements. In this process, the State authorities have primacy in defining the requirements. The ATSPs, in consultation with airspace users and airports, should develop appropriate measures to meet these requirements and additional local operations objectives stated in their Contingency Planning policy.

6.4.4 Consider legal issues

The ATSP needs to consider legal issues, including liabilities and insurance, especially in the context of cross-border provision of services during a contingency. The cross-border provision of services needs to ensure:

a) a clear definition of the applicable rules and regulations;

b) agreements have been approved by all States involved;

c) the ATSP's approved role as the aiding unit;

d) the ATSP's approved role as the failing unit; and

e) the legal framework is developed for providing ATC services in an area for which the controller may not be current or properly trained.

6.4.5 Coordinate with neighbouring States to formalize multi-State operations

Paragraph 5.4 of Attachment C to Annex 11 of the Chicago Convention recommends that, in the case of multi-State ventures, detailed coordination leading to formal agreement of the contingency plan should be undertaken with each State. Any event that limits the capacity of an ATC facility to handle normal traffic levels will impact adjacent ATC facilities, regardless of whether the situation requires transferring control of part or all of the airspace to other units. Therefore, contingency plans should be coordinated with all adjacent ATC facilities. Similar coordination should be undertaken with those States whose services will be significantly affected and with international organizations concerned.

6.4.6 Consider economics

6.4.6.1 A prime objective in defining contingency plans is to achieve adequate contingency capability at a reasonable cost. In making short-term and long-term investment for contingencies, the ATSP should consider factors such as:

a) existence of possible alternate contingency locations and systems;
b) investments and operating costs to reach a given capacity;

c) probability of an accident/failure/security breach and costs or losses incurred as a result of service disruption/unavailability; and

d) potential benefits of implementing contingency measures (e.g., lower insurance premiums).

6.4.6.2 Decision-making on investments for contingencies should also consider economic analysis. However, that economic analysis is only a part of the decision-making process in service continuity. Other factors include the binding nature of the legal framework (e.g., ICAO) and political considerations and decisions.

6.4.7 Train contingency personnel

The ATSP needs to train personnel to ensure their readiness to perform during an actual event. Contingency personnel should be trained in cross-team coordination and communication, reporting procedures, security requirements, team-specific processes and individual responsibilities. The ATSP also should ensure that contingency personnel have appropriate licenses, competencies and certifications.

6.4.8 Exercise contingency plan

The ATSP should conduct contingency-plan exercises. The exercises should simulate emergency situations and test and validate the viability of one or more aspects of the contingency plan. Issues uncovered or lessons learned during the exercises should be reviewed, investigated, and used to revise the contingency plan.

6.4.9 Generic requirements for contingency options

Table I-6-1 introduces generic considerations for a number of potential contingency strategies. These points follow a sequence of events covering the planning for system degradation to a safe and secure situation, service continuity, and recovery modes of operation. Maintenance of contingency plans is also covered.

Table I-6-1. Generic requirements for contingency strategies

Planning
• Establish requirements for contingency: — Identify key resources, including facilities management; — Ensure key personnel in ATSPs (i.e., potential failing and aiding units) are provided with means to communicate on short notice. • Liaise with sub-contractors and infrastructure providers. • Establish contingency planning group. • Ensure early engagement with Regulator/NSA as necessary. For example: — Obtain approval from regulators and State authority for procedures and practices that affect the airspace of the failing unit; — Clarify licensing and training issues when staff may be providing safety/security-related services for the airspace of a neighbouring country. • Ensure training of staff (ATCOs and ATSP) in contingency measures. • Document contingency plans. • Oversight agency to verify the existence and content of contingency plans. — In case of cross-border provisions of services during contingency, NSAs of both failing and aiding units should verify contingency plans
System Degradation to a Safe/Secure Situation
Phase 1 — Immediate Actions
A dangerous situation has been identified. Focuses on the safe/secure handling of the aircraft in the airspace of the failing unit, using all technical means still operationally available: • Secure traffic situation; • Consider evacuation of the airspace —“clear the skies” — If time permits, consult systems engineering teams and sub-contractors to determine if they can resolve a failure before this critical decision is taken. • Determine the magnitude of problem and the duration of the outage; • Prepare fall-back instructions to ensure safe/secure operations, and allow a “smooth” transition for Phases 2 through 5. • Appropriate authorities should identify the seriousness of the situation and initiate appropriate contingency measures. • Initiate process of informing all interested parties
Phase 2 — Immediate Actions
Focuses on stabilizing the situation and, if necessary, prepare for longer term contingency arrangements: • Initiate contingency measures; • Complete notification of all concerned; • Determine and coordinate flow control measures; • Initiate delegation of ATS, where appropriate.

Service Continuity
Phase 3 — Initiation of the Option
• Content depends on strategy considered.
Phase 4 — Optimization
Gradually optimize capacity up to maximum potential (within the published or reduced ICAO route and sectorization structures, in line with previously agreed end-user and regulator expectations). • Upgrade means of communication as much as possible; • Use “normal” coordination procedures as much as possible; • Consider consequences or “domino effects” on third-party ATSPs/States who will be affected by the increase in workload for the aiding units.
Recovery
Phase 5 — Longer-Term Response and Recovery
Revert to the original unit and working position in a safe, secure and orderly manner: • Initiate Transition Plan, taking into account technical and operational conditions. • Inform all interested parties of intention to revert to “normal” operations; • Assign staff between failed unit and contingency facility for “shadow” or parallel operations during transition period; • Coordinate the time at which normal operations can be resumed; • Implement updates to flight plan and radar data processing systems; • Authorize the resumption of “normal” operations.
Maintenance of Plans
• Hold immediate debrief. • Conduct a “lessons learned” exercise after actual or practice demonstrations of contingency plans. • Revise contingency planning arrangements, and promulgate changes as necessary • Ensure contingency planning is part of organization’s “change management” processes.

PART II

ATM SECURITY OPERATIONS

Chapter 1

INTRODUCTION

1.1 BACKGROUND

1.1.1 Part B provides guidance for the provision of ATM security services in support of national security, aviation security and law enforcement. Air traffic controllers are routinely confronted with aircraft that lose communications, operate with disregard for established flight rules and procedures, operate in a suspicious manner, report acts of unlawful interference in flight, or intrude into controlled airspace or security zones without permission. For these, and many other reasons, an aircraft could become a track of interest (TOI) that requires monitoring and resolution of security concerns. In addition, air traffic controllers must know what to do if military or law enforcement agencies respond to acts of unlawful interference, possible acts of aggression, or criminal activities involving aircraft in airspace under an ATSP's control.

1.1.2 Accordingly, the guidance in this part will enable the ATSP to consider the wide range of security services that the ATSP may be called upon to provide and will assist the ATSP in developing guidance pertinent to the ATSP's particular responsibilities. The ATSP will also find guidance in this part to assist in organizing to carry out the many responsibilities of ATM security operations required for strategic operations security, tactical operations security, and interagency collaboration or inter-operations security.

1.1.3 The requirements and methods for provision of ATM security services will vary among ATSPs depending upon many factors such as relationships with the military and law enforcement agencies and ATM security requirements in the National Civil Aviation Security Programme (NCASP). In recognition of this, Appendix D highlights specific national and regional examples of provision of ATM security services in Europe, the United Kingdom and the United States. Ultimately, this guidance material serves as a framework intended to assist ATSPs in providing effective ATM Security services and in structuring their organizations for efficient ATM Security operations.

1.2 INTERAGENCY COLLABORATION

1.2.1 The ATSP collaborates with many security partners when providing ATM security services. In addition to the aviation security partners identified in the State's NCASP, partners include organizations for emergency response, public health, rescue and firefighting services, customs and border security, and law enforcement organizations. Figure II-1-1 depicts the scope of ATM security services and reflects the ATSP's differing roles in supporting, safeguarding, and protection in areas of aviation security, national security, and law enforcement.

1.2.2 The ATSP should establish formal communication and coordination structures with all ATM security partners. The details of the division of responsibilities among these organizations will vary from State to State, and will depend on the differing laws, customs, and organizational structures of the government departments and agencies. The ATSP also should participate in training and joint exercises to achieve an integrated and effective response from all partners. Figure II-2-1 highlights the fact that ATM security operations could be providing for one, two or three categories of security partners at any given time through intersecting agency responsibilities.

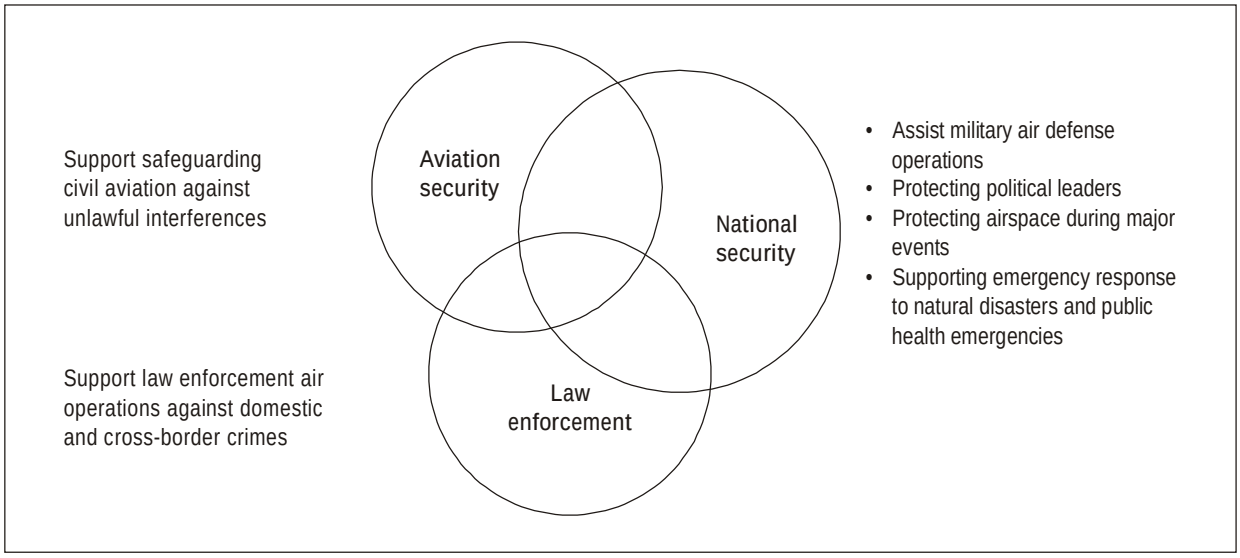


Figure II-1-1. Scope of ATSP support to security partners

1.3 SPECIAL PLANNING CONSIDERATIONS

1.3.1 This section highlights two subjects that the ATSP should coordinate with security partners to reach consensus on during the planning of ATM security operations: 1) loss of communication, and 2) tracks of interest. Both are important to the ATSP's monitoring and communicating of a flight of potential security concerns to partner organizations.

1.3.2 Loss of Communication

1.3.2.1 Some instances of loss of radio communication (COMLOSS) with ATC in recent years were associated with a security threat. COMLOSS occurs for a variety of reasons including equipment failures, human errors (e.g., switching to a wrong channel, setting the radio to very low volume), and intentional acts of malice. In a heightened security environment, prolonged COMLOSS may trigger a security related alert and potentially lead to military or law enforcement response.

1.3.2.2 The ATSP should develop policies and Standard Operating Procedures (SOPs) to monitor, identify and address the situation of COMLOSS. The initial ATC actions after COMLOSS may be, depending on agreed procedures, include:

a) to locate and display the aircraft;

b) to continue to monitor for suspicious behaviour (e.g., deviation from established procedure);

c) to continue to attempt to establish two way voice radio communications with the aircraft; and

d) to request further assistance in contacting the aircraft by:

1) using guard frequencies and/or very high frequency omnidirectional range (VOR) voice;

2) if appropriate and available, requesting that aircraft's dispatch/operations office use company voice or aircraft datalink communications channels;

3) requesting other aircraft on last assigned frequency or company frequency attempt to contact the COMLOSS aircraft; and

4) relaying the appropriate frequency via on-board phone (e.g., satellite phone), if available.

1.3.2.3 If the radio communication is not re-established after a specified duration, or because specified conditions or triggers are met, ATC may take subsequent actions based on agreed-upon protocol with the security partners and:

a) continue to monitor;

b) alert security partner(s);

c) initiate follow-up status reports at regular intervals;

d) well in advance of the aircraft crossing the ATC facility boundary, make sure that the next facility is aware of the situation and continues appropriate action; and

e) support the operation if an interception is considered necessary by the security partner.

1.3.2.4 Analysis and feedback on COMLOSS is needed to investigate the causes and to minimize future occurrence of non-security-related causes.

1.3.3 Track of Interest (TOI)

1.3.3.1 The track of interest (TOI) is used to identify a flight object of potential security concern. It is particularly useful in facilitating clear communication among security partners when there is no identification information about the airborne flight object that triggered the security attention. Normally ATC will be the first to identify a possible TOI.

1.3.3.2 Events that prompt a TOI may include but are not limited to the following:

a) non-compliance with ATC instructions, aviation regulations, applicable temporary airspace/flight restrictions, or other applicable security procedures;

b) prolonged loss of communications;

c) unusual, vague or inappropriate transmissions;

d) unusual or suspicious flight behaviour;

e) unauthorized intrusion into controlled airspace or a security identification zone;

f) unlawful interference with airborne flight crews, up to and including hijacking; and

g) notification of suspicious behaviours from adjacent Units or States or a third party.

1.3.3.3 Examples of manned and remotely piloted aircraft non-compliance with ATC instructions include: failure of the aircraft to turn on assigned transponder code, or the code changes without the aircraft being told to do so. Or, the aircraft deviates from its assigned flight/altitude and does not return to it when requested to do so. Unusual flight behaviours refer to inconsistent or abnormal manned or remotely piloted aircraft activity such as: flight over/near sites of interest; non-compliance with temporary airspace/flight restrictions; flight in prohibited/restricted airspace; inappropriate speed or rate of climb/descent; missed crossing restrictions or reporting points; pilots report flight difficulties with no or only vague explanation in response to ATC; any aircraft that requests to divert from its original destination or route for any unexplained reason, except for reasons such as: weather, company request, passenger request, mechanical difficulties, etc.; any other indicators of a suspicious situation (e.g., background noise, change in pilot's voice characteristics, etc.).

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

1.3.3.5 A TOI will normally be considered resolved under the following circumstances, as applicable:

a) the aircraft or object is no longer airborne;

b) the aircraft complies with ATC instructions, applicable aviation regulations, issued temporary airspace/flight restrictions, or security procedures;

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 or non-hostile;

e) TOI was identified based on specific and credible intelligence that was later determined to be invalid or unreliable;

f) data displayed on radar is identified and characterized as invalid (e.g., background, flock of birds); and

g) any additional information becomes available that indicates no security concern exists.

Chapter 2

ATM CONTRIBUTION TO SAFEGUARDING AGAINST UNLAWFUL INTERFERENCE

2.1 THE SECURITY ROLE OF THE ATSP IN RELATION TO OTHER ORGANIZATIONS

2.1.1 The air transportation system is an open, interconnected network system that transports both people and goods. Minimization of the risk of unlawful interference with aircraft requires a layered approach as illustrated in Figure II-2-1. Such an approach should include:

a) **Secure airport and other aviation system infrastructure:** Includes measures to prevent attacks against aircraft and ground facilities within the airport perimeter or against airport operation areas, public areas, sterile areas, remote facilities and any other aviation-related infrastructure.

b) **Secure people:** Refers to measures taken for passenger and staff screening, staff background checks, surveillance, and other access-control procedures meant to ensure that only authorized people are on board a flight or have access to the aircraft, and that they do not have prohibited articles with them.

c) **Secure baggage:** Relates to the detection and prevention of threats involving objects in the hand and/or checked baggage. These include explosives; chemical, biological, radiological, and nuclear (CBRN) materials; and other hazardous materials.

d) **Secure cargo and mail:** Relates to measures to reduce the risks from hazardous devices in cargo or mail. Such measures need to take into consideration the shipping from source to exit. The shipping chain includes cargo source, containerization, freight consolidation and forwarding, cargo and mail screening locations, air transport to destination, and all intermediate storage and transport.

Figure II-2-1. Layered aviation security

e) **Secure aircraft:** Relates to measures to reduce the risk to aircraft and the likelihood of manned or unmanned aircraft being used as a terrorist instrument. For manned aircraft, these measures may include the presence of In-Flight Security Officers (IFSO) on board, hardened cockpit and airframe, and more efficient or improved air-to-air and air-to-ground communication. For unmanned aircraft, security measures described in *Unmanned Aircraft Systems (UAS)* (Circ 328) should be applied.

Note.— The aircraft classification of unmanned aircraft includes unmanned free balloons and remotely piloted aircraft.

f) **Secure airspace:** Refers to (1) preventing a flight from taking off when advice of security concerns about the flight is received and (2) managing in-flight security events.

2.1.2 Airport operators, security providers, aircraft operators, cargo handling agents, and postal authorities have the primary responsibility for security measures pertaining to the first five security layers—securing airports and infrastructure, people, baggage, cargo and mail, and aircraft—while the ATSP, in conjunction with other aviation security partners, contributes to the layer that secures the aircraft at the airport and in the air, as well as securing the ATM system infrastructure wherever located.

2.2 ATM SECURITY FUNCTIONS FOR AVIATION SECURITY

2.2.1 This chapter sets out the general principles concerning the role of the ATSP in the management of acts of unlawful interference against aircraft. It must be recognized that despite increasingly stringent efforts to make aircraft secure, both on the ground and in the air, threats and acts of unlawful interference are likely to arise from time to time. The timing, nature, and potential outcomes of such events are impossible to predict. Response plans should, therefore, be flexible; and administrations should ensure that they take account of the critical and unpredictable nature of such emergencies.

2.2.2 As noted in the overview, the roles and responsibilities of all the organizations and agencies, including ATSPs that may be involved in the resolution of aviation security incidents are specified in the NCASP. This will include the organization with overall responsibility for managing the response to acts of unlawful interference. This may, in some States, be the appropriate authority for aviation security; in others, it may be a military agency or law enforcement authority (LEA).

2.2.3 Controllers should be aware of the general principles of security incident management and the responsibilities assigned to the ATSP under the NCASP. Although the NCASP does not dictate specific actions to be taken by the ATSP in a particular situation, it does establish the framework for ATC responsibilities and actions in relation to unlawful interference with aircraft in flight. Keeping these general principles in mind, specific ATC procedures should be developed to support aviation security.

2.2.4 Although the ATSP does not have overall responsibility for managing aviation security incidents, supporting other organizations and agencies during response to threats involving unlawful interference with aircraft requires strategic and tactical security operations. Strategic security operations must be seen and devised in the context of other agencies' agreed responsibilities and activities; the tactical security operations are those that take place in the course of responding to specific incidents.

2.3 STRATEGIC OPERATIONS SECURITY FUNCTIONS

2.3.1 Doc 8973 – Restricted requires States to develop contingency plans, at both the national and local airport level, for responding to security incidents. The ATSP should be involved in the development and periodic reviews of these plans. Detailed response plans for management of cases of unlawful interference, and other security-related events, should be incorporated in individual ATS unit local instructions. The response plans should include ATSP procedures for recovery and resumption of normal ATC operations, if an interruption occurs, after the security incident is resolved.

2.3.2 LOAs with ATS units in adjacent States should include coordination requirements and other procedures relating to aircraft subject to an act of unlawful interference that have either planned to enter the adjacent State's airspace, or may possibly divert into that airspace.

2.3.3 The contingency plans and all other documents dealing with acts of unlawful interference, including operational checklists and LOAs with adjacent ATC, should be considered restricted documents, and protected in accordance with Doc 8973 – Restricted, Chapter 2.3, and be available in all ATC facilities and facilities of relevant entities. Procedures may be disseminated on a strict need-to-know basis for such things as controller training for security operations.

2.3.4 Plans should be exercised regularly, and post-exercise reviews should be conducted to ensure staff familiarity with the procedures, and to evaluate the appropriateness of the plans.

2.3.5 The ATSP must also ensure that there are adequate facilities, and well defined coordination procedures, to permit rapid communication between ATC units, the appropriate authority for aviation security, and other organizations and agencies with responsibilities related to aviation security. All necessary contact details, including after-hours contacts where appropriate, should be readily available in all ATC facilities.

2.3.6 Contingency plans and all other documents dealing with unlawful interference, including operational checklists and LOAs with adjacent ATC should be updated prior to expiration at local and national levels.

2.3.7 All personnel involved in managing security emergencies should be aware of contingency plans and all other documents dealing with unlawful interference, including operational checklists and LOAs with adjacent ATC facilities and should be trained to cope with such emergencies.

2.3.8 The State in which an aircraft subjected to an act of unlawful interference has landed shall report the landing and transmit by the most expeditious means all other relevant information to the State of Registry of the aircraft and the State of the Operator in accordance with Standard 5.2.5 of Annex 17. These notifications would normally be the responsibility of the appropriate authority for aviation security. The ATSP will need procedures to ensure air traffic information concerning such incidents is passed to proper authorities.

2.3.9 In addition to the notifications specified above, States are required to undertake a review and analysis of all cases of unlawful interference. At the conclusion of the review, a report on the incident should be submitted to ICAO. The form of the report and details of the information to be provided are contained in Doc 8973 – Restricted.

2.3.10 While the responsibility for compilation of the report will normally rest with the State's appropriate authority for aviation security, a record of ATC actions and information received by ATC will be needed for the review of the incident and the subsequent report. The ATSP should therefore ensure that the local instructions (or similar documents) for ATS units contain appropriate provisions relating to record keeping to ensure that the necessary information will be available. Where recording of ATC frequencies and communications channels is used, the recordings covering the period of the incident should be secured for use in the review.

2.4 TACTICAL OPERATIONS SECURITY FUNCTIONS

2.4.1 An incident of on-board unlawful interference may occur if the pre-take-off preventive measures fail, requiring ATC to operate in a tactical mode to manage the incident. The acts of unlawful interference defined in Annex 17 can be grouped into the following two broad categories:

a) acts by persons on board the aircraft which jeopardize the safety of the aircraft or persons on board; and

b) actual, attempted or alleged introduction of a weapon or hazardous device on board an aircraft or at an airport, or use of ground-based weapons against an aircraft or airport facilities.

2.4.2 There will generally be significant differences in the way ATC becomes aware of these two different categories of threat. There are also differences in the handling of bomb threats compared to other forms of unlawful interference. These two categories are discussed separately in following sections.

2.4.3 This manual addresses both forms of unlawful interference primarily from the point of view of the ATSP and its responsibilities in relation to the development of contingency plans for managing incidents involving unlawful interference.

2.4.4 Monitoring and detecting possible cases of unlawful interference

2.4.4.1 ATC will often be the first to be aware of a case of unlawful interference by persons on-board the aircraft. Where possible, an aircraft that is suitably equipped should report an act of unlawful interference by transmitting transponder code 7500. To verify that it is not an inadvertent transmission, the controller should request the flight crew to confirm the selection of the squawk code in accordance with published ATC procedures.

2.4.4.2 The following are other possible means of notification for:

a) automatic dependent surveillance – broadcast (ADS-B)-equipped aircraft, selection of the ADS-B emergency mode;

b) automatic dependent surveillance – contract (ADS-C)-equipped aircraft, selection of the ADS-C emergency mode; and

c) controller pilot data link communications (CPDLC)-equipped aircraft, transmission of a CPDLC MAYDAY message.

2.4.4.3 Where selection of an appropriate transponder code, ADS mode or CPDLC message is not an option, flight crews may append the phrase “Squawking 7500” to voice transmissions immediately after transmitting the aircraft’s call sign.[1]

2.4.4.4 Where the crew is able to transmit information about the situation by voice, they may use a code to indicate the level of threat. The following are the codes defined in Doc 8973 – Restricted:

1. Older ADS-B and ADS-C aircraft equipment can only transmit a single emergency mode. The nature of the emergency will have to be established by voice or a free-text CPDLC message. Newer equipment can transmit one of five emergency modes, to indicate the type of emergency. See PANS ─ ATM (Doc 4444), Sections 8.5.4 and 13.4.3.4.5.

a) Level 1: Disruptive (suspicious or verbally threatening) behaviour;

b) Level 2: Physically abusive behaviour;

c) Level 3: Life-threatening behaviour; and

d) Level 4: Attempted or actual breach of the flight-crew compartment.

2.4.4.5 The circumstances of the unlawful interference may, in some cases, make it impossible for the crew to transmit any information about the situation on board. Controllers need, therefore, to be aware of the types of suspicious behaviour that could indicate that there has been some form of unlawful interference. The following are examples of this behaviour for manned and remotely piloted aircraft:

a) deviation from cleared flight profile without prior notification or authorization;

b) refusal or inability to comply with ATC instructions (including vectoring);

c) unusual deviation from the flight profile typical for the aircraft type;

d) loss of radio contact associated with flight profile deviation;

e) unauthorized secondary surveillance radar (SSR) code changes or extended use of the identification feature (e.g., IDENT in identification, friend or foe (IFF) system);

f) use of non-standard phraseology by the aircrew or other covert attempts to highlight the situation (e.g., a marked change in voice characteristics or a different voice);

g) non-ATC–related radio transmission (e.g., a political statement); and

h) open transmitter.

2.4.4.6 While controllers need to be alert to various indications of possible acts of unlawful interference, they should also be aware of the possibility of false alerts and should exercise caution and discretion in determining the appropriate response. Whenever occurrences such as those listed above lead to a suspicion that unlawful interference may be occurring, notifications of the appropriate authorities, as detailed in contingency plans developed in accordance with Doc 8973 – Restricted should be made. The following are factors which may affect the assessment of the situation by the appropriate authorities:

a) a manned or remotely piloted aircraft deviating towards sensitive sites inside restricted or prohibited areas or not complying with temporary airspace/flight restrictions;

b) a manned or remotely piloted aircraft in terminal airspace deviating towards significant buildings or ground facilities, even where there is no associated restricted airspace or airspace/flight restrictions; and

c) the presence on board of political figures or other high-profile individuals who could be a target of a hijack attempt.

2.4.4.7 An ATC unit may also receive information about possible acts of unlawful interference from the following external sources:

a) ATS units or States;

b) non-official sources (e.g., news agencies);

c) aircraft operators regarding on board disturbances; and

d) a non-specific threat passed via a third party.

2.4.5 Responding to Cases of Unlawful Interference

2.4.5.1 When an aircraft is subject to an act of unlawful interference, the possibly urgent nature of the act requires pertinent information to be transmitted immediately to the appropriate authority to permit the timely response for safeguarding the affected aircraft and all other aircraft likely to be affected by its operation. Therefore, as soon as circumstances indicate security precautions need to be taken, the ATS unit should transmit an initial alerting message containing all available pertinent information to the appropriate authorities, as detailed in contingency plans developed in accordance with Doc 8973 – Restricted.

2.4.5.2 In many cases, most of this information will be more conveniently obtained from the aircraft operator than by requesting it from the flight crew on ATC frequencies. However, to ensure that all available information is collected, the local ATS unit instructions (or similar document) should emphasize the need to establish a clear understanding with the other parties regarding what information each organization or agency is responsible for collecting.

2.4.5.3 Doc 8973 – Restricted lists the following essential information that should be collected and transmitted progressively to those concerned:

a) the known or anticipated route of flight;

b) the known or suspected destination and the estimated time of arrival;

c) supplementary flight plan data such as fuel endurance (expressed in hours and minutes, if possible) and the number of crew and passengers on board;

d) the composition of the flight crew and its knowledge and experience of the anticipated route;

e) the availability of navigation charts and associated documentation; and

f) flight time limitations of the flight crew, taking into account the number of hours already flown.

2.4.5.4 Additional information may be known by ATC and if available, should be forwarded:

a) call-sign, type of aircraft, registration, and operator;

b) time, aircraft position (latitude and longitude, if available), last assigned SSR code, on or off flight plan route, altitude, phase of flight (climb/descent/cruise), heading, speed, vertical rate, indication of start of turn and stop of turn;

c) flight plan information including point of departure and point of arrival;

d) pilot's intention, e.g., change of destination; expected route; assistance needed by the aircraft and aircrew: executing a rapid descent, immediate landing at a suitable airport, immediate landing at any airport;

e) current radio transmission facility (RTF) frequency and controlling agency;

f) other aircraft not responding to ATC;

g) other aircraft off route from last cleared ATC route or flight level (FL);

h) indicative factors of the aircraft's hijack status, e.g., Mode A 7500 code selection, declaration on RTF, unusual event, the nature of suspicious activity/behaviour in accordance with agreed reporting criteria; and

i) the presence of IFSOs on board.

2.4.5.5 In addition, depending on the circumstances of the event, the following information should be forwarded, to the extent that it can be obtained:

a) the number, names, and nationalities of passengers and, if possible, of the offenders;

b) the number and condition of injured persons on board;

c) the number and type and any other information on weapons, explosives, incendiary material, or other substances known or believed to be in the possession of the offenders;

d) identity of hijackers, intentions, demands from hijackers;

e) possible crash sites in range of the aircraft (threat to what by when);

f) airfields for diversion or forced landing: security capabilities; passenger management; operational characteristics, i.e., approach, apron, cross servicing agreements); and

g) the physical condition of the flight crew and, if present, IFSOs.

2.4.5.6 In handling cases of unlawful interference, controllers should do the following:

a) be discreet in communications with the flight crew and avoid overt references to unlawful interference unless it is known that the perpetrators cannot monitor the transmissions;

b) monitor the aircraft and use normal hand-off procedures without requiring transmissions or responses by the pilot unless the pilot has established normal communications;

c) if aircraft are dispatched to intercept and escort the unlawfully seized aircraft, provide all possible assistance to the intercepting aircraft to aid in placing them, initially, in a position behind and below the seized aircraft; and

d) notify/coordinate relevant information with security and defence authorities involved.

2.4.5.7 Controllers should continue to provide the subject aircraft with a normal alerting service and follow standard radio failure procedures if COMLOSS. However, they should also be alert to the possibility that the aircraft may not follow normal radio failure procedures.

2.4.5.8 Controllers must also continue to provide normal separation services to all aircraft. Particular care needs to be exercised in relation to the aircraft subject to unlawful interference, as the behaviour of the aircraft may be unpredictable.

2.4.5.9 At all times, the safety of the aircraft and persons on board should be paramount. Any requests from the flight crew regarding diversions and changes to an increased threat level should be accommodated as a matter of priority, even if this requires amending clearances for other aircraft.

2.4.5.10 If the flight crew advises they are diverting the aircraft to an airport other than the intended point of landing, or if it appears from the aircraft's behaviour that this is a possibility, the aerodrome control unit at that airport should be advised as soon as possible so that they may implement the appropriate measures specified in the airport emergency plan.

2.4.6 Bomb threats

For simplicity, this section will use the term bomb threat in a generic sense to encompass threats from devices, weapons or substances. In addition, the threat could also be a threat to attack an aircraft or ATC facility rather than placing such a hazardous device on the aircraft. Similar procedures apply to all these types of threats.

2.4.7 Bomb threats and dealing with threatening calls

2.4.7.1 The methods by which threats involving bombs or other hazards may be received and the information they may contain vary considerably. They include phone, email or other forms of Internet-based messaging, or a written note left in a prominent place. The initial information may be received from one or more of, for example, the aircraft operator, an ATC unit, the media, LEA, etc. The information may be specific to an aircraft or ATC facility or it may be a more general threat. It may refer simply to "a bomb," or it may give specific information about the type of bomb or other hazardous device.

2.4.7.2 If the message is received by phone, it may be possible to obtain additional information by judicious questioning, as long as the caller can be kept on the line.

2.4.7.3 Many telephone systems have the ability to trace calls, even after the caller has hung up, provided that the line has not been closed at the receiving end. The ATSP should ensure that where this capability is available, that it is implemented for all phones in ATS facilities.

2.4.7.4 The ATSP should ensure that all staff who are likely to answer calls to publicly available numbers are aware of the procedures for dealing with threatening calls and that this is included in recurrent training.

2.4.8 Responding to bomb threats

2.4.8.1 The initial actions in response to a threat depend on how the information is received. Where the advice of the threat is not received by an ATS unit, it is important to obtain and record the name and contact details of the person passing on the advice and to establish who else has already been notified.

2.4.8.2 The threat must be assessed and classified as genuine or hoax and should be detailed in the contingency plans in accordance with Doc 8973 – Restricted. If the threat is assessed as genuine, it will be classified as either specific, if it refers to a particular aircraft, or non-specific, if it is of a more general nature. The credibility and likelihood of the threat must also be assessed –usually on a Red, Amber or Green basis.

2.4.8.3 In all cases of a credible threat to a specific aircraft, an alert phase should be declared immediately and the appropriate rescue coordination centre notified.

2.4.8.4 The response by ATS to a bomb threat depends on the stage of flight at the time of receipt and should be consistent with Appendix 40 of Doc 8973 – Restricted.

2.4.8.5 If the aircraft is on the ground prior to departure, the air traffic controller should initially deny any request for a take-off clearance (or cancel it if already issued) and immediately notify supervisory staff. Supervisory staff should then follow established procedures to notify the operating company, the airport authority, and the appropriate aviation security authority as designated in contingency plans (except where it is known that one or more of these bodies are already aware of the situation). If necessary, the aircraft should be directed to the designated isolated parking position or, if that is not available, to another suitable isolated position in accordance with the procedures specified in the local Airport Emergency Plan.[2]

2.4.8.6 Take-off clearance should be issued only if the threat has been declared a hoax or the aircraft has been searched and the appropriate authority has determined that no threat exists.

2.4.8.7 If the aircraft is airborne, the pilot in command will generally, in consultation with the aircraft operator, require priority handling for landing as soon as possible. Controllers should provide all possible assistance in expediting the flight and accommodating requests from the pilot.

2.4.8.8 Where feasible, consideration should be given to keeping the aircraft clear of heavily populated areas. However, the safety of the aircraft and its occupants must always be the first consideration.

2.4.8.9 The control tower at the aerodrome of intended landing should be notified of the situation as soon as possible. The tower controller should alert the rescue and fire fighting service, implement the relevant procedures in the local Airport Emergency Plan, and give the subject aircraft priority for landing and taxiing to the isolated parking position.

---

2. The isolated parking position is described in Annex 14 — *Aerodromes*, Section 3.14.

Chapter 3

ATM SUPPORT FOR LAW ENFORCEMENT

3.1 OVERVIEW

3.1.1 The ATSP may be requested by LEAs to assist their operations through special handling of airspace and air traffic, or provision of information related to specific flights. Law enforcement operations could include local activity such as police using helicopters and RPAs to stop or monitor an illegal activity on the ground or to support an enforcement operation against cross-border criminal activity. If security-related airspace/flight restrictions are needed, the ATSP should follow procedures to establish temporary airspace/flight restrictions. The dimensions and times of use of temporary airspace/flight restrictions should be the minimum required for containing the expected activities, taking into consideration the safety requirements of the LEA air operations and regular flight operations.

3.1.2 Depending on the State's guidance, the ATSP may also assist ground interdiction and response efforts by law enforcement personnel to unlawful interference on-board an aircraft, or other illegal activity including the targeting or shooting of civil aircraft in flight with small arms fire, lasers, or man-portable air defence systems (MANPADS) or illegal use of unmanned aircraft systems. Often, this entails ATM personnel providing "monitoring in the air" until the LEAs on the ground assume responsibility after the aircraft has landed. ATSP support to LEAs could also include providing flight plan information on request such as country of registry, operator, origin and destination. Often an agency other than an ATSP is tasked to detect and provide surveillance of aircraft suspected of drug smuggling across the border or overland. However, the ATSP could have corollary roles in support of such surveillance efforts.

3.2 LASER THREATS

3.2.1 Laser beams can cause temporary blindness or permanent damage to human tissues, especially the retinas. The distance over which laser pointers can be used ranges from 2,000 feet to well over 20 miles. When pointed directly or even indirectly at a pilot or an air traffic controller, some lasers could cause eye injury or temporary visual impairment such as flash blindness and distraction and may lead to a catastrophic outcome. Additional information regarding the hazardous effects of laser emitters is available in the *Manual on Laser Emitters and Flight Safety* (Doc 9815).

3.2.2 To protect flight operations from being adversely affected by laser beams, ICAO established related SARPs in Annex 14 recommending the establishment of protective zones around aerodromes. The ATSP supports enforcement of these zones by reviewing applications of light shows or other operations which may emit lights that potentially endanger flight operations.

3.2.3 High-powered, inexpensive lasers are widely available, and laser incidents have become a significant safety and security concern. The ATSP should continually track the intentional use of lasers against aircraft and analyse the trend of laser incidents. To enable this process, Doc 9815, 5.6, recommends that Contracting States, that may wish to establish an incident-reporting system, provide a means of monitoring unauthorized use of lasers in airspace. Rapid notification of an incident will assist in the investigation and possible enforcement action against the offender. Samples of incident report formats are provided in Doc 9815, Appendix B.

3.2.4 When the ATSP receives an initial laser report from the pilot, the ATSP should ensure that the following information is recorded:

a) time of the event;

b) aircraft ID;

c) aircraft type;

d) colour of laser (red or green, etc.);

e) position/location — fix/radial distance, approach to specific runway, nearest town, miles and direction from an airport, or latitude–longitude, etc.;

f) altitude;

g) aircraft's direction during the incident;

h) position of the laser in relation to the aircraft;

i) cockpit illuminated — Yes/No;

j) flight crew injuries — Yes/No;

k) flight crew visually hindered by visual effects (such as glare, flash blindness, loss of dark adaptation, glare discomfort and afterimage);

l) flight crew's intentions (e.g., continue/go around);

m) LEAs notified — Yes/No (name and phone number, if available);

n) brief description of the event; and

o) other pertinent information.

3.2.5 The ATSP should maintain a complete and accurate account of the event for an agreed period of time after the proper investigating entity is notified.

3.2.6 States should establish laws and regulations to prohibit the intentional use of lasers against aircraft and impose penalties for violations. The ATSP should encourage air traffic controllers to work with the pilots and LEAs in identifying the origin of laser beams used against aircraft and provide assistance as required to LEAs in locating and identifying suspects.

3.3 MAN-PORTABLE AIR DEFENCE SYSTEM (MANPADS) THREATS

3.3.1 MANPADS represent a significant threat to civil aviation. Because of their portability and sophistication, MANPADS are difficult to detect and are capable of causing catastrophic damage to even large civil aircraft. Many MANPADS are lethal to approximately 15 000 feet from a distance of 5 miles or more. The following section defines alert levels for MANPADS threats and procedures for reporting MANPADS events.

3.3.2 The ATSP should work jointly with State and civil authorities to create a strategic plan and procedures for response to MANPADS events.

3.3.3 MANPADS threats can be classified using alert levels.

a) Alert Level 1 — Increased awareness, operations normal;

b) Alert Level 2 — A credible threat to a specific airport, carrier or region. Review contingency/mitigation plans (if any); and

c) Alert Level 3 — Observed or reported launch — implement any contingency/mitigation plans.

3.3.4 Alert Level 1 response. Alert Level 1 represents the lowest MANPADS alert level to a MANPADS threat. Increased vigilance and recognition by the ATSP is a key element in preventing or limiting an attack. ATC personnel who believe a suspicious activity exists or is imminent should notify their supervisors for further action.

3.3.5 Alert Level 2 response. A MANPADS alert Level 2 should be implemented following receipt of information concerning a credible MANPADS threat to a specific airport, airline, or region. This information should be relayed to the appropriate LEAs and State defence agencies, as required.

3.3.6 Threat-level information from MANPADS activity should also be communicated, consistent with SARPs and strategic response plans and procedures to:

a) the appropriate aircraft operator operations centre;

b) the ATC facility controlling the specific flight;

c) the adjacent ATC facilities; and

d) the ATC tower of the affected facility or facilities.

3.3.7 Alert Level 3 response. Alert Level 3 should be implemented after an observed or reported attack. When a MANPADS launch is observed by the ATC facility or reported to the ATC facility by any aircraft under its control, an initial report of information should be prepared by the ATSP, including:

a) call sign (if known);

b) type of aircraft (if known);

c) coordinated universal time of the attack;

d) position/location;

e) altitude; and

f) any other pertinent information.

3.3.8 The ATC facility supervisor receiving the report or witnessing the attack should ensure the information is communicated to the appropriate LEAs, State defence agencies and civil authorities, as required.

3.3.9 MANPADS information should be broadcast on the affected airfield automated terminal information system (ATIS) in accordance with ATSP and civil aviation procedures.

Chapter 4

DISASTERS AND PUBLIC HEALTH EMERGENCIES

4.1 ATM SUPPORT FOR DISASTER RESPONSE AND RECOVERY

4.1.1 The response and recovery effort following manmade or natural disasters almost always involves some form of air operations that necessitate ATC services. In some cases, the ATSP may be unable to provide air traffic services because aviation infrastructure may be damaged or destroyed. In other instances, ATC infrastructure may be unaffected but special ATC security services may be required during the response and recovery from the disaster. Examples of such ATC security services include services for surveillance flights to determine the extent of damage, rescue operations, airlift of personnel and supplies, and evacuation of injured persons. In the case of wild fires, fire-fighting aircraft will be involved. In some situations, RPAs may be used for surveillance of disaster areas and for other disaster-related purposes. RPA use for such activity may require implementation of special ATC procedures. Media organizations also have legitimate roles during disasters that may require special ATC procedures for their aircraft. Very Important Person (VIP) flights by high-level State officials for surveillance or visitation may require security coordination and temporary airspace/flight restrictions.

4.1.2 This chapter reflects the broad view described in Doc 9854 that ATM Security also includes security issues associated with unintentional threats. These include human error and natural disasters or hazards that destroy parts of the ATM system and that require ATM security emphasis to ensure the security of the ATM system as it recovers. This also provides specific ATM security services in support of national security and law enforcement actions following such hazards or unintentional threats. Although Aviation Security is based on intentional threats, Aviation Security is only one aspect of ATM Security. Both intentional threats and unintentional threats and hazards must be considered under ATM Security.

4.1.3 Because there are often intensive flight operations in the disaster zone, the relevant authorities will often request the ATSP to restrict the type, and possibly the number, of aircraft operating in the area. This requires use of temporary airspace/flight restrictions. The extent of the restrictions and the types of operations to be permitted should be established in coordination with the authority responsible for the disaster response. The information should be published in a notice to airmen (NOTAM).

4.1.4 The ATSP's contingency plan should identify the appropriate organizations with which coordination will be needed for the types of crises and disasters likely to be encountered. It should include contact details (including after-hours contacts). Where there is advance knowledge of an impending crisis or disaster, coordination with the appropriate local, State, and national authorities can be initiated in advance; however, in some circumstances, this will not be possible. The system, therefore, needs to be capable of reacting quickly to requests for support for crisis and disaster response operations.

4.1.5 During the event, the ATSP should ensure that only authorized aircraft are given permission to operate within airspace restricted for crisis management and disaster recovery operations and, as appropriate, provide priority handling for aircraft authorized to support crisis management and disaster relief operations. The length of time that the airspace/flight restrictions are needed should be determined by the authorities responsible for the response effort. If the operations continue over an extended period, the extent of the airspace restrictions and the restrictions on the types of flights permitted should be reviewed periodically.

4.2 COMMUNICABLE DISEASE AND OTHER PUBLIC HEALTH RISKS ON BOARD AIRCRAFT

4.2.1 In the globalized world, diseases can unintentionally spread far and wide via international travel and trade. A health crisis in one country can spread rapidly to another. Early identification of potential cases of communicable diseases and other public health risks among air passengers is an essential component in reducing the likelihood of such cases resulting in a widespread pandemic public health emergency that could have national security consequences.

4.2.2 In addition, no country is immune from the threat of terrorism; and there is ongoing concern over the threat of CBRN terrorism with its effects spread through the use of exposed or infected people on-board commercial aircraft. The potential for intentional spread of diseases and other public health risks through people on-board aircraft presents a national security and aviation security threat that requires ATSP awareness and action to support medical authority procedures and potential law enforcement or military action and intervention. Therefore, ATM services required in Chapter 16 of Procedures for Air Navigation Services — *Air Traffic Management* (PANS-ATM, Doc 4444) for such issues is properly included in this manual as an ATM security service.

4.2.3 Preparedness planning for a possible CBRN public health related event should include communication and collaboration between the national and local public health and security agencies in advance of the identification of such a threat, in order to facilitate an efficient response.

4.2.4 The International Health Regulations (2005) of the World Health Organization (WHO) specify the procedures for responding to cases of suspected communicable diseases on board aircraft. Implementation of the majority of these procedures is the responsibility of public health authorities, airport operators and airlines.

4.2.5 Airlines are required to provide guidance for cabin crews in the identification and on board management of potential cases of communicable diseases. The provisions of Annex 9 — *Facilitation* and Section 16.6 of the PANS-ATM, Doc 4444 require the flight crew to notify ATC as soon as any possible cases of communicable diseases or other public health risks are identified.

4.2.6 The following information is required:

a) aircraft identification;

b) departure aerodrome;

c) destination aerodrome;

d) estimated time of arrival (ETA);

e) number of persons on board;

f) number of suspected case(s) on board; and

g) nature of the public health risk, if known.

4.2.7 The PANS-ATM (Doc 4444), Section 16.6, also requires that an ATS unit, upon receipt of such advice of communicable disease or public health risk on-board and aircraft, shall forward this information, as soon as possible, to the ATS units serving the destination and departure unless procedures exist to notify the appropriate authority designated by the State and the aircraft operator or its designated representative.

4.2.8 The cabin crew generally will not be in a position to identify a particular disease or CBRN effect. They will most likely be limited to providing only a description of the observed symptoms. To aid the medical authorities in their assessment of the response required, these descriptions should be recorded exactly as advised by the crew.

4.2.9 The PANS-ATM (Doc 4444), Section 16.6, further states that when a report of a suspected case of communicable disease or other public health risk on board an aircraft is received by the ATS units at the destination and departure aerodromes, either from another ATS unit or from an aircraft or an aircraft operator, they are required to forward a message, as soon as possible, to the public health authority or other appropriate authority designated by the State, to the aircraft operator or its designated representative, and to the local airport operator.

4.2.10 Following the initial notification, the airport operator should be advised of any changes to the ETA of the aircraft.

4.2.11 States should not deny entry to an aircraft because of a reported case of a possible communicable disease. Article 28.1 of the International Health Regulations (2005) does, however, specify that should the intended point of entry not be equipped for applying the appropriate health measures required under the regulations, the aircraft may be required to divert to a more suitable aerodrome of entry, provided that this option is operationally feasible.

———————

Chapter 5

AIRSPACE MANAGEMENT FOR ATM SECURITY

5.1 MONITORING AND REPORTING OVER SECURITY IDENTIFICATION ZONES

5.1.1 The Contracting States, within airspaces in their sovereignty, have legal authority to allow or deny access to their sovereign airspace, in accordance with Chicago Convention provisions. The national laws should designate which national authorities and agencies have responsibilities for: establishing rules and procedures for the use of airspace; allowing or denying access to national airspace; and resolving issues related to diplomatic clearances and national security (e.g., air defence) requirements. The ATSP may be required to support these security requirements by monitoring and providing information about flights over security identification zones.

5.1.2 A designated security identification zone is the airspace over a specific area of sovereign land or water where the control of aircraft is necessary for national security. Security identification zones are typically over the territorial boundaries and are designed to protect the air sovereignty of the State. Aircraft operations within security identification zones are restricted to those that meet specified requirements. These requirements may include maintaining two-way radio communications with ATC, filing a flight plan containing the time and point of the security identification zone penetration, squawking a discreet code, reporting altitude, and departing within a specified time of the estimated departure time. These requirements must be consistent with the agreements among the CAA, the State's military authority responsible for national defence, and the State's agency responsible for border security.

5.1.3 The ATSP should notify the aviation community through NOTAMs, the Aeronautical Information Publication, and other official communication channels of security-related requirements pertaining to flights entering, exiting, transiting, or operating within the nation's territorial airspace. The ATSP acquires, processes, and disseminates flight plan information to the relevant aeronautical facilities. The monitoring and reporting of aircraft movement information should be consistent with the procedures specified in each ATC facility standards operating procedure (SOP).

5.1.4 In some instances, the ATSP may detect a non-compliant aircraft within a security identification zone. After detecting a non-compliant aircraft, the ATSP should notify the appropriate air-defence organizations according to the facility SOP, and the aircraft should be declared a TOI.

Note.— In some areas, the use of primary radar could be necessary for identifying visual flight rules (VFR) aircraft and ensuring VFR aircraft are compliant with applicable requirements.

5.1.5 In certain situations, the ATSP could be notified of a non-compliant aircraft by the State's defence or security organizations. The ATSP should locate and display the aircraft on the air traffic monitoring system. In addition, the ATSP may assist in identifying and tracking the aircraft, and may be asked to announce to security partners the position, altitude, airspeed, and direction of flight. The ATSP also should notify the affected ATC facility along the path of the TOI to coordinate the tracking of the unknown aircraft until it lands. Consistent with any agreements that may be in place with the CAA, State military authorities and civil agencies, the ATSP should notify the designated authority when the aircraft lands.

5.1.6 In an emergency situation, the pilot-in-command, for the safety of the flight, may need to deviate from the rules. The ATSP should take into consideration the safety of the flight and security requirements and advise the Pilot-in-Command to change the flight path accordingly.

5.1.7 If an aircraft must be intercepted, Annex 2 — *Rules of the Air* (Section 3.8) must be followed:

> 3.8.1 Interception of civil aircraft shall be governed by appropriate regulations and administrative directives issued by Contracting States in compliance with the Convention on International Civil Aviation, and in particular Article 3(d) under which Contracting States undertake, when issuing regulations for their State aircraft, to have due regard for the safety of navigation of civil aircraft. Accordingly, in drafting appropriate regulations and administrative directives, due regard shall be had to the provisions of Appendix 1, Section 2 and Appendix 2, Section 1.
>
> *Note.— Recognizing that it is essential for the safety of flight that any visual signals employed in the event of an interception which should be undertaken only as a last resort be correctly employed and understood by civil and military aircraft throughout the world, the Council of the International Civil Aviation Organization, when adopting the visual signals in Appendix I to this Annex, urged Contracting States to ensure that they be strictly adhered to by their State aircraft. As interceptions of civil aircraft are, in all cases, potentially hazardous, the Council has also formulated special recommendations which Contracting States are urged to apply in a uniform manner. These special recommendations are contained in Attachment A.*
>
> 3.8.2 The pilot-in-command of a civil aircraft, when intercepted, shall comply with the Standards in Appendix 2, Sections 2 and 3, interpreting and responding to visual signals as specified in Appendix 1, Section 2.

5.2 EMERGENCY SECURITY CONTROL OF AIR TRAFFIC

5.2.1 States may want to develop an emergency preparedness plan that prescribes actions to be taken by appropriate national authorities in the interest of national security to control air traffic under emergency conditions. A plan for emergency security control of air traffic would define the authorities, responsibilities, and procedures to identify and control air traffic within a specified area during air defence or national emergency conditions. ATM, airspace, and security measures and required roles of the ATSP should be identified in the plan.

5.2.2 When national authorities decide to impose emergency security control measures on air traffic, national protocols to implement emergency security control of air traffic would be followed.

5.2.3 The restriction of air traffic in response to an attack or a threat to national security could be accomplished by implementing coordinated and appropriate airspace control measures. Agreed upon control phases or measures requested by national or military authorities and implemented through the ATSP, might include, but are not limited to: specific air routes, specific corridors, specific flight and aircraft operator authorizations, flight planning and procedural restrictions, or the selective or systematic shutdown of specified airspace.

5.2.4 Emergency security control of air traffic could be implemented in phases to facilitate a smooth transition from normal air traffic identification and control procedures to the more restrictive identification and control procedures needed for the situation. The airspace control measures within each phase could be changed, adapted, or deleted, as required. Airspace control measures could also be implemented without the use of these phases, if the situation dictates. Agreed upon phases could follow a pattern of application to security identification zones, specific air corridors, and all areas under control of the ATSP.

5.2.5 Aircraft missions' assigned priorities in the State's emergency security control of air traffic plan could have specific flight plan requirements, could require squawking of discreet transponder codes, could require direct radio communications with an ATC facility, and could require entry of specific security related information in the remarks section of the flight plan. Specific security information required in the flight plan could be included with the flight plan data and could be passed from one ATC facility to the next and to the appropriate air defence control facilities.

5.2.6 Situations could occur that cannot be controlled in accordance with an emergency air traffic priority list of requirements. Aircraft emergencies and inbound international flights that have reached the point of no return, including international aircraft operator flights en route to safe haven airports in accordance with specific international agreements, are examples of such situations. These events should be treated individually through coordination between the ATSP and appropriate military authorities in consideration of the urgency of the in-flight situation and existing tactical military conditions.

5.2.7 There may be occasions when aircraft would need to fly but will not be able to because the aircraft has no priority or the aircraft's proposed route-of-flight conflicts with the imposed flight restrictions. On these occasions, provisions for a special flight approval request should be available and followed.

5.2.8 Upon receipt of a properly authenticated message implementing emergency security control of air traffic, the ATSP should do the following:

a) implement airspace control measures as directed;

b) disseminate emergency security control of air traffic implementation instructions to all ATC facilities within the ATSP's area of jurisdiction and advise adjacent ATC facilities that may be impacted; and

c) notify national authorities when the emergency security control of air traffic measures are accomplished or estimated to be accomplished.

5.2.9 After implementation of emergency security control of air traffic measures, the ATSP should coordinate directly with national authorities for changes or modifications.

5.2.10 Air traffic controllers, upon notification of emergency security control of air traffic measures, should do the following:

a) broadcast appropriate security instructions on all frequencies at State-specified intervals on all available frequencies until instructed otherwise; and

b) comply with all airspace control measures as directed by ATSP officials.

5.3 CREATION, PROMULGATION AND MONITORING OF TEMPORARY AIRSPACE/FLIGHT RESTRICTIONS

5.3.1 Each Contracting State should identify the authorities entitled to require the creation of temporary airspace/flight restrictions and the circumstances under which temporary airspace/flight restrictions may be created. The CAA should promote appropriate ordinary or urgent procedures for the establishment, publication, and implementations of such temporary restrictions. Examples of circumstances that may necessitate the use of temporary airspace/flight restrictions are large sporting events, head of State travel, affairs of State, events of national importance such as international summits, and crisis/disaster response.

5.3.2 Events requiring temporary airspace/flight restrictions generally occur with some prior notice to the ATSP, usually resulting in a pre-planned approach to event management. The ATSP supports the decisions of competent authorities by helping to define, from a technical standpoint, the operational impact on air transport and related operations at airports and airspace in order to meet security requirements with facilitations, as suggested by Annex 17, Section 2.3.

5.3.3 NOTAMs for temporary airspace/flight restrictions should be issued, in accordance with Annex 15 and may contain the following:

a) reason for the temporary airspace/flight restrictions (unless classified);

b) definition of the airspace volume;

c) effective time and the expiration time (perhaps “until further notice”); and

d) operating instructions defining requirements for flights that can operate within the airspace, procedures for how they must operate, and any specific aircraft or flights that may not operate within the airspace during the period of the temporary airspace/flight restrictions.

5.3.4 After the temporary airspace/flight restrictions have been defined fully and coordinated with security partners, the ATSP activates the temporary airspace/flight restrictions and notifies security partners and other airspace users of the temporary airspace/flight restrictions for use in their flight planning. This is accomplished through a published NOTAM.

5.3.5 During the period when the temporary airspace/flight restrictions are in effect, procedures for detailed actions, roles, and responsibilities for monitoring the temporary airspace/flight restrictions should be followed, depending on the Contracting State’s organization and with respect to tasks allocated for air policing. Procedures should also be provided for priority communication links and coordination for activating engagement rules for TOIs.

5.3.6 Temporary airspace/flight restrictions should be cancelled as soon as possible.

———————————

Chapter 6

ORGANIZING FOR EFFECTIVE ATM SECURITY OPERATIONS

6.1 OVERVIEW

6.1.1 Standard 3.5 of Annex 17 of the Convention on International Civil Aviation requires Contracting States to require ATSPs 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. ICAO Doc 8973 – Restricted, Chapter 17, "Crisis management and response to acts of unlawful interference", provides guidance for ATC response in the instances of unlawful interference. These plans are detailed in the NCASP for each State.

6.1.2 As explained in the previous chapters, ATM security services address an even broader range of security threats that are diverse, dynamic, and often time sensitive in nature. To effectively execute the security mission, the ATSP should, to the extent possible, make provision for security services in an agile and integrated manner through practices that include tactical security operations, strategic security planning and operations, and interoperation agreements with its security partners. This chapter presents a suggested organization of operations and activities along these functional lines, consistent with the requirements of Annex 17 and the broader ATM security mission (Figure II-6-1).

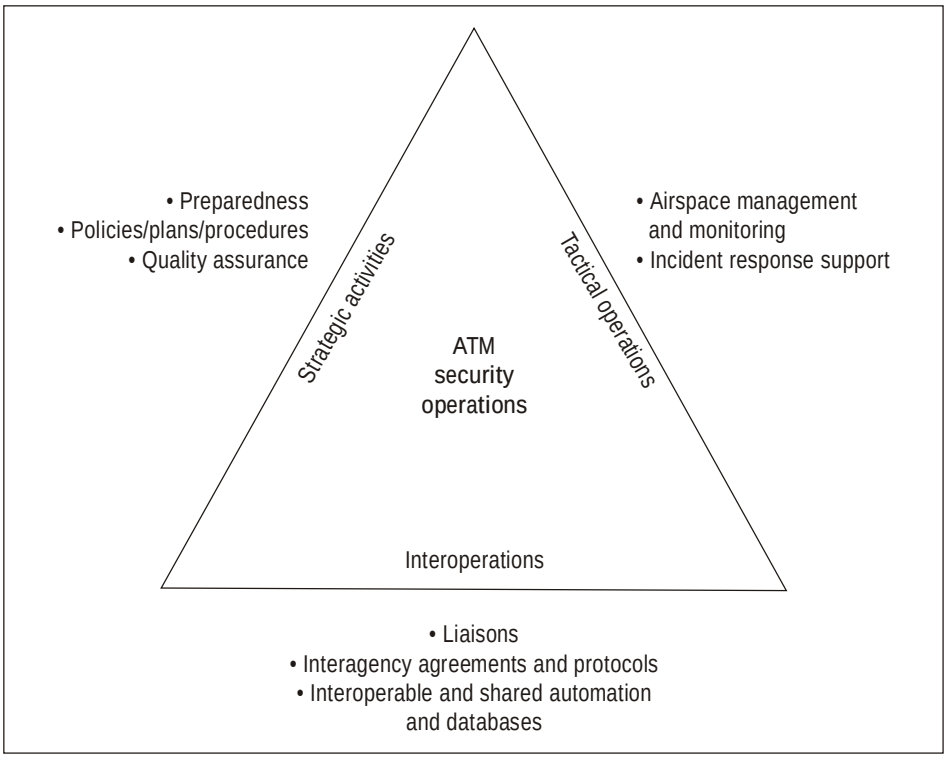


Figure II-6-1. ATM security operations: tactical, strategic and interoperations

6.1.3 Organizing ATM security operations functions as shown in Figure II-6-1 would enable the ATSP to ensure a proper focus and balance on the needs of each security area as follows:

a) strategic security activities and operations that strengthen the continuity of the ATM system via long-range planning, crisis management, procedure development, support functions, and analysis;

b) tactical security activities and operations that provide daily ATM security oversight of ATM system operations to facilitate maximum awareness of and immediate response to security situations; and

c) interoperation agreements and activities that support interoperability and collaboration with external security partners such as State defence or law enforcement agencies, and enhance cooperation and coordination through imbedded liaison.

6.2 STRATEGIC SECURITY PLANNING AND OPERATIONS

6.2.1 Interagency planning and preparedness is the process of facilitating collaboration and cooperation with State and defence agencies for the purpose of pre-planning the ATSP's role in providing ATM security services for national security, aviation security, and law enforcement. Interagency planning and preparedness are key strategic elements that permit the execution of integrated and comprehensive State plans involving ATM security operations.

6.2.2 Plans should include coordination with State authorities and, if necessary, local authorities. In addition, national defence and/or military authorities responsible for airspace security, as designated in the NCASP, should be consulted. Plans should include emergency preparedness, analysis of law enforcement and intelligence information and employment of technologies to assist in the detection of threats and vulnerabilities.

6.2.3 However, the strategic component of ATM security operations is also concerned with pre-planning and preparation for crisis management operations, development of ATM security operations procedures, and ATM security operations support.

6.2.4 This section highlights items that should be considered under each aspect of strategic security functions.

6.2.5 Interagency planning and preparedness should focus on the following issues and activities:

a) establishing a threat response plan that directs the operational response to disasters and any source of intentional threats or attacks that involve the ATM system;

b) defining strategies to mitigate the operational and economic impact of an attack or disaster that would have a major negative impact on the ATM system;

c) defining measures that will enable the ATM system and other affected critical government and private sector aviation-related elements to recover quickly from an attack or disaster;

d) conducting strategic planning and coordination with international ATM organizations and military organizations to optimize the continuity of ATM security, especially between adjacent ATM systems;

e) preparing ATM security plans related to the following:

1) the outbreak of a communicable disease on board an aircraft from intentional or unintentional causes that poses a public health risk or public health emergency of international concern;

2) airborne interception;

3) on-board law enforcement response;

4) aviation law enforcement ground interdiction and response;

5) ATM support for counterterrorism operations;

6) interdiction and disposition of designated TOIs; and

7) domestic attack or threat of attack, including threats using standoff weapons such as MANPADS;

f) development and implementation of a national plan for aviation security:

1) a risk-based approach should be used to develop and implement measures to reduce vulnerabilities and impacts of associated threats on the ATM system;

2) plans should identify ATSP responsibilities for coordination with State and local authorities during emergency situations, provide for ATSP access to law enforcement and intelligence information, and describe expectations of ATSP employment of technologies to assist in the detection of threats and vulnerabilities; and

3) plans requiring ATSP airspace management services for ATM security should include coordination with military authorities responsible for airspace security.

6.2.6 Crisis management operations support should focus on the following issues and activities:

a) coordinating and managing the ATM system emergency planning activities for the ATSP;

b) developing ATSP contingency plans in preparation for natural disasters, military conflicts, or acts of unlawful interference with civil aviation:

1) these can affect ATM system capabilities for civil aircraft operations and the provision of air traffic and supporting services; and

2) the plans should provide for the immediate deployment of appropriate personnel and assets;

c) collaborating with appropriate agencies on plans for national, regional, and local exercises to ensure the operational readiness of ATM security capabilities and the mitigation of impacts of these exercises and related measures on the safety and efficiency of the ATM system;

d) planning ATM security exercises that include tactical level aviation threat scenarios:

— in addition to testing the coordination among ATSP command and control functions, the exercises should incorporate realistic scenarios involving actual aviation assets and facilities; and

e) establishing crisis response reporting capabilities that reflect the status of ATSP employees, ATM system services, equipment, and other key ATM infrastructure.

6.2.7 Security operations procedures and support involves preparation of ATM security procedures to counter, control, resolve or defeat threats to the ATM system and to support military and law enforcement operations in the ATM system and should include some or all of the following:

a) developing detailed operational plans and security procedures for synchronizing the respective responsibilities identified in the plans of the involved agencies:

— this will include plans to identify and respond to aviation security threats on board aircraft including reports of threat levels, possible or confirmed hijacking, terrorists equipped with improvised explosive devices (IEDs) or weapons of mass destruction, pandemic diseases, management and handling of suspicious situations/behaviour, etc.;

b) preparing procedures to categorize and identify designated flights of interest that do not represent an immediate threat to the national interests but do require focused attention, coordination, and potential response;

c) developing procedures for establishing, activating, using, and deactivating security-related airspace/flight restrictions within the ATM system wherein limitations may be imposed upon aircraft operations;

d) developing surveillance and alerting procedures for airspace affected by temporary airspace/flight restrictions when violations of restrictions resulting in TOIs are predicted or witnessed;

e) ensuring ICT security policies and procedures to handle classified and sensitive information are followed:

1) various agencies and departments are involved in classified aviation operations and sensitive programmes that enhance the security of a State; and

2) to achieve this support, specific individuals from the CAA/ATSP should have appropriate levels of security clearances and should be trained on classified and sensitive programmes to support the needs of other agencies and departments;

f) planning for the infrastructure required to properly support ATM security operations;

g) providing programme management for the development of surveillance and tracking systems that would enable faster security identification of potential airborne threats in territorial airspace;

h) enhancing crisis management integration through automated surveillance tools and systems that support interagency continuity of operations;

i) implementing quality assurance programmes that focus on ATM security data collection and analysis at the national, regional, facility, and individual levels:

— quality assurance also involves providing specific guidance on facility standards, investigation, reporting, and recording of security incidents that impact the ATM system;

j) collecting and analysing aviation security data; establishing and maintaining data for security-related information (such as TOIs and laser incidents) and their associated impact on the ATM system;

k) regularly assessing ATM security plans and programmes using quality-assurance derived data, and coordinating necessary updates to ATM security plans with other departments and agencies; and

l) making sure ATM security operations procedures comply with safety risk management (SRM) requirements.

6.3 TACTICAL SECURITY OPERATIONS

Tactical security operations by ATSPs support the daily management of security operations in the air domain through real-time (or near real-time) coordination with other security partners. ATSP functions pertaining to tactical security operations may include some or all of the following:

a) efforts to detect, deter, and defeat threats to the ATM system; to reduce vulnerabilities; and to minimize the consequences of, and expedite the recovery from, attacks that might occur;

b) identification of real-time ATM security-related events;

c) immediate tactical operational response or assistance, if appropriate, to State authorities to properly respond to TOIs. Response or assistance to State authorities may include any of the following activities, and the role of the ATSP in these activities should be included in the NCASP:

1) airborne interception and surface-to-air operations by State authorities;

2) on-board law enforcement response;

3) aviation law enforcement ground interdiction and response by State authorities; and

4) airspace management initiatives in support of State counterterrorism and law enforcement operations;

d) operational response to protect the ATM system during an attack, or threat of attack, including attacks using standoff weapons such as MANPADS;

e) gathering, processing, and furnishing air movement data to the proper air defence facilities:

— this is in accordance with mutually acceptable procedures for all flights of civil and military aircraft requiring identification in security identification zones and temporary airspace/flight restrictions;

f) initiating appropriate coordination within the ATSP promptly upon receiving notification or other information that an incident is occurring and that an immediate response is required. This protects the ATM system from any associated threat or when immediate ATM security services are required in support of authorities responding to the incident;

g) notifying the aviation community, consistent with appropriate agreements between the CAA and the defence department, of ATM security-related requirements pertaining to flights entering, exiting, transiting or operating within the ATSP's airspace or operating in airspace affected by temporary airspace/flight restrictions. Notification methods may include NOTAMs, official Internet sites, or other methods;

h) coordination and support for critical aviation security stakeholders during tactical security-related activities and incidents involving the ATM system. Coordination may be conducted in a variety of ways such as using open communication lines, or on-site collaboration at key State agency or defence facilities:

— this includes the establishment, condition, or change in any aeronautical facility, service, procedures, or hazard which could be ATM security-related;

i) assigning air traffic security coordination responsibilities to personnel at key facilities that are involved in monitoring ATM security and identifying TOIs, and initiating appropriate tactical actions and communications regarding ATM security events. Personnel designated with air traffic security coordination responsibilities should be responsible for or have oversight of the following:

1) response to aviation security related incidents such as violations of temporary airspace/flight restrictions, reports of unlawful interference on board an aircraft, reports of unruly passengers and associated threat levels, reports concerning State-designated special-interest flights, stolen aircraft, identification of TOIs, etc.;

2) collaboration with security partners to develop security-related airspace/flight restrictions and NOTAMs and to ensure the timely distribution of the information to reduce or mitigate the impact that the measures have on ATM system operations;

3) negotiating, designing, building and publishing security-related airspace/flight restrictions;

4) receiving, processing and distributing VIP itineraries;

5) receiving, processing and publishing all requests for vetting of flight operations in accordance with temporary airspace/flight restrictions;

6) developing, refining and publishing security-based NOTAMs and special notices; and

7) retrieving, organizing and compiling resources associated with disasters, both natural and man-made.

6.4 SPECIAL INTEROPERATIONS SECURITY FOR CIVIL, MILITARY AND LAW ENFORCEMENT OPERATIONS

This function establishes a close working relationship with military and law enforcement organizations to accomplish the following:

a) provide ATM security interface for sensitive/classified operations in the ATM system such as VIP movements and major political or sporting events (e.g. G-8 Summit, Olympics, World Cup);

b) provide ATM security interface for military users of the ATM system, particularly those responsible for intercept of TOIs;

c) provide ATM security interface for government agencies and law enforcement agencies responsible for air domain security operations;

d) provide classified and unclassified ATM security-related interaction as appropriate to support national defence and aviation security missions and to permit appropriate ATM actions to mitigate the impact of national security-related procedures on the ATM system;

e) establish liaisons with appropriate security clearances who can participate in conferences and in the coordination of air defence activities with civil and military agencies;

f) cooperate with State and regional or local law enforcement agencies to provide ATM security-related support for law enforcement missions;

g) develop recommendations to enhance and clarify interagency efforts to monitor and vet flights, within the ATM system, for compliance with security and other requirements levied on air operators;

h) coordinate a comprehensive interagency communication plan for emergency security control of air traffic:

— all State agencies with a role in aviation security should be able to communicate with each other for mutual response to emergencies and to take full advantage of shared situational awareness;

i) identify and implement, if appropriate, protective airspace security measures for all events requiring use of security-related airspace/flight restrictions;

— preliminary advisories should be published prior to the event, in accordance with CAA procedures, and periodic reviews of ATM security measures for these events should be conducted;

j) serve as the CAA point of contact for managing relationships and ATM security responsibilities among State departments, agencies or other entities:

1) pre-arranged agreements such as Memorandums of Understanding (MOUs) or Memorandums of Agreement (MOAs) will help in coordinating operations where there are shared resources and interdependent responsibilities;

2) clarify understanding of each party's commitment and purpose regarding ATM security;

3) prepare responses to established criteria regarding operational issues, breaches of the original commitment, or the purpose of the MOUs and MOAs; and

k) provide outreach and education regarding security-related procedures and airspace/flight restrictions. ATM security liaisons and staff specialists could assist the CAA in conducting periodic visits to airports, flying clubs and fixed-base operators to increase pilot awareness of security-related airspace/flight restrictions and to reduce the number of non-compliant aircraft that become TOIs.

6.5 ATM SECURITY OPERATIONS ADMINISTRATION

6.5.1 All the functions described above — Strategic security operations; tactical security operations; and special interoperations security — could administratively reside in an ATM security operations office. The ATM security operations office would serve as the nexus between security operations and the ATM system. This office could provide a centralized focus on the many ATM security responsibilities of the ATSP and improve integration of security operations within the State's airspace.

6.5.2 The functions of the ATM security office would be to:

a) manage the CAA/ATSP's ATM security efforts to protect the State and its interests from threats related to international and domestic civil aviation operations and disasters;

b) mitigate the impact of any threats on the ATM system and assist with associated government response measures (such as temporary airspace/flight restrictions) on the safety and efficiency of the airspace users; and

c) provide effective ATM security operations through cooperation with the external security partners (military, emergency response, law enforcement, and other ATSPs).

APPENDICES

Appendix A

SECURITY RISK MANAGEMENT PROCESS

1. INTRODUCTION

1.1 Entirely eliminating risk is not possible; therefore, when managing security risks, ATSPs should take a risk-informed approach. This document refers to risk management as the process of assessing risk and the selection of risk mitigation options by considering the associated costs and benefits of the actions taken. Risk management provides a structured approach for ATSPs to make rational decisions regarding the risks.

1.2 Effective security risk management does not operate in a vacuum but needs to consider the context in which the ATSP operates. To ensure a layered and comprehensive approach to aviation security, ATSPs should closely collaborate with other stakeholders including aviation authorities, other national agencies, and security service providers.

2. SECURITY RISK MANAGEMENT PROCESS

2.1 The security risk management process is comprised of a number of interrelated elements, and is an on-going, iterative activity. Figure App A-1 outlines a high-level view of the process that ATM organizations can follow to systemically identify security risks and mitigation options. This methodology is applicable to the whole organization and to a specific component or facility.

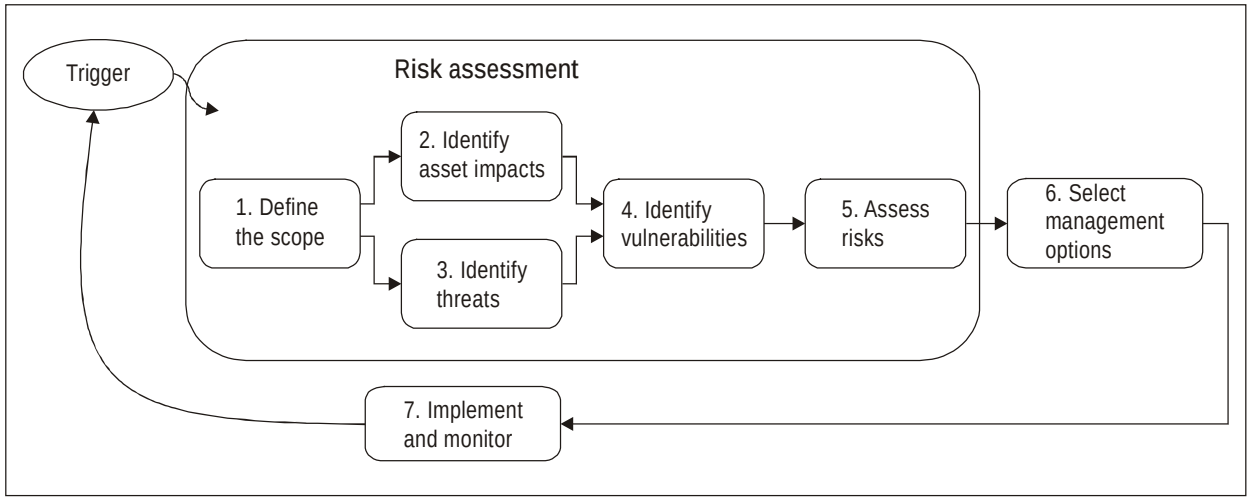


Figure App A-1. Security risk management process

Triggers

2.2 The risk management process should be an ongoing, iterative activity. ATSPs should identify triggers for risk management to ensure that the security management of the ATM system is updated continuously and meets the challenges posed by the changing environment. ATSP may conduct security risk assessments as scheduled events or when triggered by changes in key factors affecting the risk posture of the ATM system. Common triggers include:

a) change in threat environment (either threat types or frequency of occurrence);

b) security incident (e.g., an attack that reveals an unexpected vulnerability);

c) change in security policy that may affect change in risk priorities or risk appetite; and

d) change to the ATM system or development of a new ATM system.

2.3 Risk management process consists of seven steps:

— Step 1: Define the scope

— Step 2: Identify asset impacts

— Step 3: Identify threat agents and likelihood of attacks

— Step 4. Identify vulnerabilities

— Step 5: Assess risks

— Step 6: Select risk management option

— Step 7: Implement and monitor

2.4 Steps 1 to 5 are often referred to as the risk-assessment process, which serves as the foundation for identifying, evaluating, and selecting mitigation measures in Step 6. Step 7 implements the selected mitigation measures and monitors their effectiveness to provide feedbacks.

Step 1: Define the Scope

2.5 The objective of this step is to ensure that the scope of the ATM system to be assessed is understood. The ATM system includes several components: people; information; technology; facilities; services; and CNS. The scope often may be a subset or a complete set of these assets.

2.6 This step is accomplished through first defining the boundary of the ATM system to be assessed, followed by documenting security goals, and concluded with developing a description of the ATM system/subsystem.

2.7 The system boundary description should include the following information for the ATM system (or subsystem) to be assessed:

a) system components;

b) operating environment;

c) users, their roles and authority;

d) third parties associated with the ATM system, including organizations, their roles, and authority;

e) essential supporting services or infrastructure, including security infrastructure and assumptions about its quality or security;

f) services provided by the assets and associated security obligations (including services and obligations to third parties);

g) lifecycle phase of the ATM system (or sub-system) to be assessed (e.g., design, deployment operations, maintenance, out of service); and

h) legal and regulatory requirements.

2.8 After the system boundary and interfaces are defined, the ATSP should identify assets within the system boundary and provide an architectural description of the system to allow the identification of potential threat paths (vulnerabilities) between access points and assets.

2.9 Security goals are particular to the ATM system/subsystem being assessed. They need to be specific enough to relate to groups of assets and types of security incidents.

Step 2: Identify Asset Impacts

2.10 This step evaluates the consequence of potential security events on assets within the scope. The impacts may be measured as:

a) safety;

b) efficiency/effectiveness;

c) financial/economics;

d) public confidence; and

e) political.

2.11 Impacts are described in a qualitative scale with the minimum level being “negligible.” Often a four-point scale above negligible is adequate. The following is an example scale for impacts on operational efficiency:

0 Negligible—Loss is expected to cause negligible effect on the organization's performance.

1 An asset may be affected in such a way that the organization's performance will be detected to be below a tolerable standard. This should include situations where the maintenance of the service is lost for a substantial time.

2 Loss of a group of assets will cause a cessation of service. This may be the result of losing a group of similar assets or losing a string of sequential systems. It also applies to stopping operations if another incident occurs before the asset can be operationally restored or the loss mitigated.

3 Loss of asset will cause an immediate reduction in capacity and will negatively impact ability to deliver the required service.

4 Loss will cause immediate cessation of the service.

Step 3: Identify Threats

2.12 This step identifies the threat agents and assesses the likelihood of events.

2.13 ATSPs should consider a broad range of threats. They may vary by nature of intent such as intentional threats (e.g., criminal, terrorist), unintentional (e.g., accidents), and natural disasters (e.g., floods). Threats may also vary depending upon the agent (e.g., external or internal to the organization).

2.14 It is important not to overlook internal threats. For ICT systems, internal threats are the greatest threat for cybersecurity. Every legitimate point of access is a potential source of attack. This includes users/operators of the system, other organizations with remote access or some degree of dependence on the system, and necessary system services. These are extracted from the boundary description and listed as potential threat agents.

2.15 External threat agents include terrorists, criminals, extremists, enemies, naturally occurring hazards, and service degradation (e.g., power failure). Intentional threats include various methods of attack such as bombing, chemical, biological, radiological and nuclear (CBRN) attacks, cyberattacks, and electronic and magnetic attacks (e.g., spoofing, jamming).

2.16 Threats should be organized according to asset types. Some examples of threats to different asset types include:

a) physical and personnel assets: Threats to physical assets (facilities) and personnel include extreme weather, natural disasters, IED, and CBRN threats, blackmail, kidnapping, extortion;

b) ICT assets: Threats to an organization's data or knowledge that may be further characterized as threats to integrity, confidentiality and availability. There are significantly more threats to ICT systems than to physical systems;

c) procedural assets: Threats to documentation and policies that result in deleted, missing or corrupted documentation.

2.17 Once the lists of potential threat agents have been identified, identify the likelihood of attacks.

2.18 Each threat requires an estimate of the likelihood that the threat will result in an attack being attempted by an adversary. For other hazards, threat is estimated as the likelihood that a hazard will manifest itself. In the case of natural disasters and accidents, the ATSP may have available statistics.

2.19 For intentional threats, particularly terrorist threats, the ATSP may not have the expertise or resources, and will need to seek advice from intelligence or security agencies. It often is difficult to quantify the likelihood of attack after intentional threats; therefore, qualitative assessments from domain experts should be used. Similar to the impact scale, it is acceptable to have a short qualitative scale, ranging from 0-5, with the lowest score being “negligible”.

Step 4: Identify Vulnerabilities

2.20 Vulnerabilities are system or operating procedure features that may be exploited by attackers or are susceptible to a natural hazard (e.g., hurricane). For example, physical assets may not have adequate fencing, security guards or surveillance systems; personnel may not be properly trained in security procedures; ICT systems may not have adequate antivirus protection; and procedural assets may have inherent vulnerabilities such as poor (or poorly communicated) documentation, lax practices or poor staff vetting.

2.21 Attackers seek the easiest path into a system. Therefore, when assessing vulnerabilities, it is important to look across all paths. For example, when assessing the risk to ICT, it is important to consider the vulnerability of non-ICT elements of the system (e.g., failure to address security education, which may allow a social engineering attack via a system administrator).

2.22 The likelihood of an incident depends on the vulnerability of the system. Therefore, the assessor must consider the security controls that have been implemented along the threat path, and determine how much these controls reduce the vulnerability to an attack. The vulnerability to a particular threat, the likelihood of a threat producing an attack, and the associated impacts are used for determining risk.

Step 5: Assess Risks

2.23 The purpose of assessing risk is to develop a comprehensive risk picture for the ATM system. A risk is a potential for an adverse outcome and is expressed as a function of threat likelihood, vulnerabilities, and impacts.

2.24 All valid combinations of threats (attacks) and system vulnerabilities should be considered to determine if a path through the asset or system exists that would allow an attack to succeed. Risks can then be assessed by considering the likelihood of the threat (attack) or hazard, the vulnerability of the asset or system to that type of threat, and the impact or consequences of loss or degradation of the asset or system.

Step 6: Select Management Options

2.25 This step identifies and selects management options for risks that have been identified. It is accomplished through the following activities:

a) determine if the identified risks are acceptable:

– This determination is based on the ATSP’s risk tolerance level or risk appetite as established in the security policy. The security policy should have specified this in terms of both risk level and impact level. The inclusion of impact level, in addition to the risk level, is to allow the ATSP to be aware of risks that are unlikely but have devastating impacts.

b) identify management options:

– Management may take any of the following actions for risk above acceptable level:

1) tolerate (do nothing);

2) treat (apply control measures to reduce it to an acceptable level);

3) transfer (transfer to another unit within the ATSP or an outside entity); and

4) terminate (stop activity);

c) select control options:

– Control options are countermeasures designed to mitigate risks. Security controls may be technical, procedural, or based on policy. These controls also cover a spectrum of activities, depending upon their approach to interrupting the threat paths. They can deter threat attacks, decrease the likelihood of a successful attack by reducing vulnerabilities, lessen the consequences of attacks or disasters, enable rapid reaction and emergency response to an incident, or allow the ATSP organization to resume normal operations effectively through contingency planning.

Moreover, the selection of control option may be considered in a larger context of the ATM system/sub-system being assessed, or external to the ATSP organization. For example, a NAVAID facility located inside the airport perimeter may leverage the airport access control measures.

d) prioritize the mitigation actions:

– The prioritization effort is to inform resource allocation decisions. A comprehensive risk picture coupled with control options provides the basis for the ATSP management to establish infrastructure protection priorities. The evaluation and selection of management options depend upon factors such as statutory and regulatory requirements, acceptability, feasibility, and cost. For example, the ATSP may define an action-triggering threshold. For any asset or system with a risk above this triggering level, mitigation options would be implemented. However, ATSP management could also prioritize risk mitigation actions for systems with a risk level below the action-triggering threshold based on cost effectiveness considerations. The security team, domain experts, and senior management should jointly make final risk management decisions with the concurrence of the regulatory agencies.

Step 7: Implement and Monitor

2.26 The ATSP should monitor to evaluate the effectiveness of the mitigation measures after their implementation. If the performance of implemented measures falls short of the expected goal, the ATSP should take corrective measures. Evaluation and correction drives continuous improvement of the risk mitigation programmes. With this activity, the ATSP receives feedback on whether the implemented mitigation measures are correctly executed and meet the anticipated performance. The actual performance provides a basis for establishing accountability, facilitating diagnosis of the performance gap, and enabling revision of goals and objectives. Monitoring performance also warns the ATSP of early indicators for areas of potential concerns and allows for proactively prevent failures from happening.

3. SECURITY RISK MANAGEMENT — ORGANIZATIONAL COLLABORATION

Intelligence-led Security Risk Management

3.1 Annex 17 encourages international cooperation and the exchange of information and intelligence on threats. Standard 3.1.3 specifies that “Each Contracting State shall keep under constant review the level of threat to civil aviation within its territory, and establish and implement policies and procedures to adjust relevant elements of its national civil aviation security programme”.

3.2 The identification and assessment of security risks is strongly dependent on information. This information can come from different sources and backgrounds including historic data analysis, emerging threats and attack patterns.

3.3 ATSPs (especially those in non-government ownership) will have limited access to all relevant information.

3.4 States and appropriate national/ regional intelligence organizations should exchange relevant information with ATSPs concerning the threats to aviation and air navigation and emerging attack capabilities or patterns.

3.5 With Amendment 12 to Annex 17, States are further required to share the relevant part of the NCASP with the ATSP.

National/local Aviation Security Committee(s)

3.6 Under Annex 17, Contracting States are required to establish a national civil aviation security committee (or similar arrangement) to coordinate the security activities between the departments, agencies and other organizations of the State, airport and aircraft operators, ATSPs and other entities concerned with or responsible for the implementation of various aspects of the NCASP. This is the principal platform for the coordination of aviation security measures.

3.7 On a similar note, airports must also designate an authority for coordinating security procedures and establish an airport security committee at each airport to assist the authority. These local working arrangements extend the national platform.

3.8 Although the ATSP may not always be located at or within the vicinity of an airport, the ATSP should make use of these platforms. Effective organizational collaboration and coordination requires the involvement of all actors in these working arrangements.

3.9 The appropriate authority should designate the ATSP to the relevant national/ local aviation security committee(s) or establish a new committee for the collaboration and information exchange with the ATSP.

3.10 The collaboration should also include the amendment of the respective local emergency plans (including designation of local emergency operations centre and relevant coordination procedures) to include responses to attacks on ATM infrastructure, facilities and services.

———————

Appendix B

CYBERSECURITY IN ICT SECURITY

1. INTRODUCTION

1.1 "Cyber" is a prefix used to describe a person, thing, or idea as part of the computer and information age, such as "cyberspace," the electronic medium in which online communication takes place. The ATM system architecture is continuing to evolve into an open architecture of interconnected cyber systems using standard data transmission protocols and open source operating systems. The civil aviation community is increasingly dependent on cyber information and communication technology (ICT) to carry out missions and business functions and the interconnectivity of cyber systems is also increasing, both on the ground between stakeholders, and between systems on the ground, aircraft, and space (global positioning systems).

1.2 While this technology evolution increases the efficiency of the operations, it also exposes the information and communication systems to higher cybersecurity risk. Cybersecurity commonly refers to the safeguards and actions that can be used to protect the cyber domain from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cybersecurity strives to preserve the integrity and availability of the networks and infrastructure and the confidentiality of the information contained therein.

1.3 Cyberattacks on ICT systems are constantly occurring with growing volume and sophistication, and the safety of passengers, crew and ground personnel could be endangered in the event that ATM ICT systems are tampered with. Additionally, ATSP employee personal information should be protected against unauthorized access and use.

1.4 This chapter provides concepts and definitions for cyber ICT security and includes a description of security requirements for ATSP critical cyber ICT systems based on Doc 8973 – Restricted. A general ICT Security guidance based on European Union (EU) requirements is shown in Appendix C and provides a comprehensive ICT security control catalogue.

2. CONCEPTS AND DEFINITIONS

Cyber ICT Assets

2.1 ATSP cyber ICT assets include the information/data,[1] information technology systems, and communication technology systems.

2.2 Information assets include operational information and employee personal information that are generated, processed or transmitted by the ATSP. Operational information is the information relevant for the provision of air traffic services. It also includes information exchanged between the ATSP and its security partners such as national or regional

1. In this appendix no differentiation is made between the term "data" and "information."

aviation security agencies, national security and defence agencies, and law enforcement agencies. Some of this security information may be classified.

2.3 Cyber-information technology systems include both software and hardware. Software includes operating systems, applications and data processing. Hardware includes computing devices, computer systems, processing systems, and data storage devices and systems.

2.4 Cyber-communication technology systems refer to networks of communication devices and systems. These networks may be local, regional, or worldwide, and wired or wireless.

Cyber ICT Security Objectives

2.5 Cyber ICT security refers to the application of security controls to protect ATM cyber-ICT systems against the degradation of integrity, confidentiality and availability from intentional or accidental causes:

a) *Integrity* is a security objective that ensures information and systems are not modified improperly or accidently. 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.

c) *Availability* is a security objective that ensures the reliability and accessibility of data, services, and resources 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.

2.6 To safeguard ATM ICT systems, it is also necessary to address the security of the environment in which these systems function. Therefore, ICT security is also concerned with physical security, suppliers, infrastructure services, and third parties that the ATSP interacts with, such as law enforcement, security, and regulatory authorities.

Cyber ICT System Criticality

2.7 Criticality is generally defined as the degree to which an organization depends on the information or ICT system for the success of a mission or of a business function. In the context of this manual, criticality is expressed in terms of the ATSP mission:

— the provision of ATM services, including the support to national/ regional security incident management.

Cyber ICT Security Controls

2.8 Security controls are safeguards or countermeasures implemented to protect the integrity, confidentiality and availability of ICT assets. Security controls may be organized into the following three classes:

a) management controls are controls that focus on the management of security risk and the management of system security;

b) operational controls are safeguards or countermeasures that are primarily implemented and executed by people; and

c) technical controls are safeguards or countermeasures that are primarily implemented and executed by the system through mechanisms contained in the components of the system.

3. CYBER ICT SECURITY REQUIREMENTS

3.1 This section is based on Doc 8973 – Restricted, Chapter 18, “Cyber threats to critical aviation information and communication technology systems”. This document recommends that States require aviation industry operators (including ATSPs) to identify security measures for critical cyber ICT systems. Therefore, the ATSP should implement these measures as the minimum ICT security requirements. The original text is modified slightly for addressing the ATSP as its audience.

Identify Critical Cyber ICT Systems

3.2 The ATSP should identify critical cyber ICT systems software and hardware used in their ATM system infrastructure, which may include, but are not limited to:

a) ATC system assets or components;

b) security command, control and dispatch systems;

c) access control and alarm monitoring systems;

d) closed-circuit television surveillance systems;

e) regulated agent and/or known consignor databases; and

f) portable and non-portable electronic devices that are used for processing, storing, and communicating critical ATSP information (e.g., desktop computers, laptop computers, netbook computers, tablet computers, mobile phones built on mobile computing platforms, personal data assistants, digital cameras, and media storage devices including universal serial bus media storage devices and memory cards).

Protection of Critical Cyber ICT Systems

3.3 The ATSP should implement cyber ICT security measures for the identified critical cyber ICT systems according to the NCASP and relevant national programmes. The objectives of these measures should be, at a minimum:

a) to protect the systems against unauthorized access and use;

b) to prevent tampering with the systems; and

c) to detect attacks on the systems.

3.4 The physical protection of such systems should begin at the design stage or as early as practicable to ensure that they are as robust as possible against cyber-attacks. This may be achieved using a multi-layered approach, which includes, but is not limited to:

a) management controls, such as:

1) security standards, policy and procedures;

2) appropriate recruitment, selection and training of staff, particularly persons with administrator rights, including background checks;

3) threat and risk assessment to determine the vulnerability of a system and likelihood of attack;

4) quality control, including inspections and tests; and

5) hardware and software supply chain security;

b) virtual or logical controls, such as:

1) firewalls;

2) data encryption;

3) network intrusion detection systems; and

4) anti-virus systems;

c) Physical controls, such as:

1) ensuring system hardware, particularly servers, is appropriately secured and located in areas to which access is controlled;

2) implementing authentication systems verifying that only those authorized to have access are accessing the system, such as biometric log on methods and/or passwords;

3) limiting the number of persons with authorized access;

4) requiring more than one person for access approvals to critical systems;

5) continuous monitoring and control of access to systems;

6) using remote backup systems in the event of loss of the primary system; and

7) maintaining activity logs, which can be useful in auditing and evaluating, as well as providing alerts when there is activity outside of normal operating parameters.

3.5 The protection of critical cyber ICT systems should be included in the risk assessment processes established by the appropriate authority. This may be achieved by including critical cyber-ICT systems in assessments of likely threats (attacks), vulnerabilities, and impacts or consequences of loss of the cyber-ICT system.

3.6 The ATSP should establish measures to mitigate potential cyber-attacks, and verify the implementation of such measures as part of their regular compliance monitoring activities, such as inspections and audits.

4. SECURITY MEASURES FOR CRITICAL CYBER ICT INFRASTRUCTURE

Security by design

4.1 The ATSP should ensure that security measures are included in the design, implementation, and operation of new cyber ICT systems, including the disposal of hardware and software. Modifications to existing systems should also take into account security to the extent practicable.

4.2 The ATSP should also include cyber security provisions in the specifications for and procurement of new cyber ICT systems. Suppliers to these systems should be required to provide details as to how information on and operation of the system is secured, including arrangements for on-going support and maintenance, whether on-site or from remote locations.

4.3 Preventative maintenance should be scheduled and managed, and if support and maintenance is outsourced, the number of individuals permitted access to system software and hardware should be limited. Such a measure will help prevent unauthorized access to the system and minimize the opportunity for individuals to interfere with the integrity of the system.

4.4 Similarly, routes for cables should be designed so that critical aviation ICT systems cannot be easily infiltrated.

Network separation

4.5 The ATSP should ensure that networks used for critical cyber-ICT systems involved in ATC are separated from networks that allow public access.

4.6 The software and hardware of a modern ICT system are inoperable without the necessary cables and connectivity to another operational system network to facilitate data transmission and exchange. For that reason, cyber ICT systems should be examined to ensure that security objectives are not compromised by exposing them to uncontrolled or open-access communications networks. Appropriate policies and practices should be in place to reduce the number of connections to the minimum required. This practice is often referred to as “hardening”.

4.7 Cyber connections to networks should take place under controlled conditions, where the type of information, and frequency or method of data exchange between the system and the network is known. An effective management system for these network interfaces should be established to ensure that all connections to a system are documented, reviewed, and upgraded as necessary and that adequate virus and malware protection is in place, where applicable.

4.8 Additionally, a layered approach to software management should be considered. A limited number of individuals should have administrative rights to a critical cyber ICT system. Access to such a system should be based on the principle of legitimate need. For example, some individuals may be granted read-only rights, while others may be granted access only to parts of the system relevant to their specific tasks.

Remote access

4.9 The ATSP should ensure that remote access to critical cyber ICT systems is only permitted under pre-arranged and secure conditions, and that suppliers do not have unauthorized access to such systems after they have been procured and/or installed.

4.10 In most instances, remote access requires that suppliers have a means of accessing a cyber-system. The ATSP should ensure that this access route is known to them, and that the method and conditions of entry are agreed upon. For example, the supplier should be required to notify a designated official from the operator whenever access to the system is needed. Alternatively, an automatic email message should be generated to notify the designated official from the operator each time access is sought.

4.11 Maintenance of cybersystems should be performed by authorized personnel only, and at pre-arranged and approved times. The ATSP should request suppliers to limit the number of persons authorized to provide support and maintenance to the system. Background checks should be conducted on such persons, including criminal history to the extent legally permissible.

4.12 The above measures should be complemented with an appropriate audit and exception-reporting system generating an automatic report whenever there is abnormal activity in the cybersystem, such as access to the system outside of normal operating hours. For example, should entry be sought outside of pre-arranged hours, an exception report should be sent to a supervisor with responsibility for the system. The supervisor should follow-up with the supplier to determine why entry was necessary without prior agreement. Similarly, audit logs should be reviewed regularly to identify and follow up on exceptional access.

Supply Chain Security for Hardware and Software

4.13 Cyber ICT systems need to be upgraded from time to time due to changes in operating requirements or software upgrades, and often require modifications in software and/or hardware. In each of these circumstances, there is a possibility for the unauthorized introduction of software or hardware that can attack, infiltrate, or compromise the integrity of the system.

4.14 ATSP should implement measures to ensure that only reputable and legitimate suppliers are used to procure hardware and software for cyber ICT systems. The concept of supply chain security should be applied to the extent practicable. The objective of this measure is to ensure the integrity of software and hardware is protected against unauthorized interference throughout the supply chain. Suppliers should be required to provide details of their security measures, not only at the installation stage, but also over the lifetime of the system.

Cyber Security Incident Records

4.15 Understanding the threat and the likely methods of attack are key elements in developing appropriate security measures to safeguard cyber ICT systems against cyberattacks. The ATSP should implement a reporting regime for cybersecurity incidents and include such regimes in the ATSP security programmes.

Evolving Considerations

4.16 Cyber ICT security will play a greater role in the next generation ATM systems, such as NextGen in the United States and SESAR in Europe. As cyber ICT system data communication links replace existing voice communication channels, there is a greater need to ensure that data links using security controls are timely and reliable, as they will be vital to the success of the programmes.

4.17 SWIM provides the opportunity for sharing ATM data such as meteorological, air traffic flow, flight trajectory, and surveillance through cyber ICT systems. The timely, secure, and reliable delivery of the ATM data through the cyber ICT system is paramount to the success of next-generation ATM systems.

Appendix C

ICT SECURITY CONTROLS

1. INTRODUCTION

1.1 The material in this appendix was developed by EUROCONTROL to assist ATSPs in Europe in implementing the regulatory requirements for ICT security. The guidance was developed by taking into consideration the following two issues:

a) the need to assist organizations in selecting the appropriate controls from the large number specified in the international standards; and

b) the wide range of ATSP organizations and the ICT system types.

1.2 To address these issues, this guidance includes a catalogue of ICT security controls (Table App C-1 to Table App C-10). This catalogue is based on the compilation and consolidation of the following international standards:

a) all relevant standards for information communication security in ISO/IEC 27001:2005; and

b) other relevant standards, particularly from COBIT and the ISO/IEC 13335-4 family.

1.3 The catalogue also incorporates best practices to ensure practical and up-to-date applications of these standards. By following the guidance, the ATSP organization will be compliant with the prevalent international standards.

1.4 In addition, the ICT security controls are organized into six levels, depending on the risk of information systems designated by the organization. Level 1 is lowest risk and requires the lowest level of baseline control; Level 6 is the highest risk and requires the highest level of baseline control.

2. CONTROL CATEGORIES

The ICT security controls are organized into nine categories according to the organization's functions.

1) *Organizational Direction and Policy Controls*

The organizational direction and policy controls deal with the collections of people, external entities, and organizations that adhere to security policies and procedures of a given organization.

The security policy is a document that is approved by management, distributed to all employees and external entities, covers all systems, and describes the responsibilities of each party relevant to the usages of the systems covered by the policy. It is a living document that undergoes scheduled review cycles and unplanned updates, as needed, to ensure the currency and effectiveness of the contained policies. The security policy is also part of the risk management approach for assessing and managing ICT security.

2) *Organization, Culture, and Management Controls*

The successful development and deployment of a policy-based ICT security system is dependent largely on management participating and supporting the effort with clear and continued commitment to the process.

The controls provide a mapping of organizational operations objectives to security objectives with well-defined management roles and clear ICT security objectives.

3) *Human Resources Controls*

Human resources ICT security controls relate to employees and contractors, and their roles, responsibilities, and suitability. Risk is examined and reduced by ensuring that they are properly screened and trained for their roles. Of concern are the inherent risks of theft and resource misuse.

4) *Physical and Environmental Security Controls*

Physical and environmental ICT security controls are concerned with the use of a facility's location, security perimeter, access control techniques, and various security equipment to protect an organization and its ICT assets.

5) *Operation of ICT Systems Controls*

Operation of ICT systems controls ensure that operational security, defined in procedures and policies, is properly implemented. Education of system users helps to ensure that policies are understood and obligations are fulfilled.

6) *Technical Mechanisms and Infrastructure Controls*

Technical mechanisms and infrastructure controls ensure that appropriate network configuration controls provide sufficient network protection, and that selected technical controls prevent unauthorized entities from accessing system data.

The principle of least privilege is typically used to ensure that an individual or system is not granted more access than needed to perform their task.

Examples of controls consist of firewalls, intrusion detection systems, access control lists, data encryption, passwords, network segregation, and routing control.

7) *Acquisition and Development Controls*

Acquisition and development controls are ensured through the use of proven system engineering methodologies making sure that security is fully integrated into all the phases of the acquisition and development lifecycle.

8) *Monitoring and Audit Controls*

Monitoring and audit controls are concerned with security logging of events, audit logs, and fault logs. System alerts and alarm monitors are employed to detect alert conditions and unauthorized system use.

9) *Compliance Controls*

Compliance controls ensure that systems comply with statutory, regulatory, and contractual agreements and requirements. Controls are typically ensured through system audits.

Categorizing the controls by organizational functions allows different functional parts of an organization to relate to a smaller group of controls. However, this does not mean that organizational risk management can focus on a single organizational function to protect particular asset; usually controls will be needed from several functions.

3. LEVEL OF CONTROLS

3.1 ATSP organizations vary in size and types. For example, ATSPs in Europe can range from being an organization with a small staff providing a limited range of service (e.g., NAVAIDS) to those managing sophisticated ATC centres. In some States, it is the government agency that provides air traffic services through a wide variety of ATM systems or facilities.

3.2 To accommodate the range of these ATSP organizations and the ICT systems, the security controls are further grouped into six levels of increasing rigour. The key differentiator is the risk level of an ATM ICT system. The risk level varies according to the criticality of the service provided by the ATSP organization, the vulnerability of the ICT system, and the nature of threats.

3.3 The six control levels: Level 1 to Level 6 are cumulative and correspond to the baseline ICT control requirements for ATM organizations. Each control level has an increasing degree of ICT complexity or ICT assets of increasing risks. For example, Level 1 is the lowest level and is appropriate for an organization with a limited and isolated ICT system. Level 6 is the highest level, which would demand a competent implementation of all the control requirements (Level 1 to 6) and is appropriate for a national defence or intelligence organization. The key differentiator is the risk level of an ICT system. The risk level varies according to the criticality of the service provided by the ATSP organization, the vulnerability of the ICT system, and the nature of threats. The general characteristics for each control level are summarized in Table App C-1, while the detailed description of each level for each of the nine organization functions is provided in Tables App C-2 to App C-10.

3.4 Within each table, the control levels are described in ascending order from Level 1 to Level 6. It should be noted that these levels are cumulative in nature, that is, the higher level controls contain all of the lower ones in addition to what is specified for the level.

3.5 The control levels have been devised so that an organization with “balanced” security will have a similar control level in each of the organizational functions. An ATSP may wish to review its ICT security posture by assessing the control level for each of the nine categories. This self-assessment may indicate areas where the controls are inconsistent in their levels. Figure App C-1 illustrates how control level may provide a convenient means to visually identify areas for attention. In this illustration, the target is Level 2. The control levels for each of the nine categories indicate that audit and organization are at Level 1 controls and does not meet the required baseline.

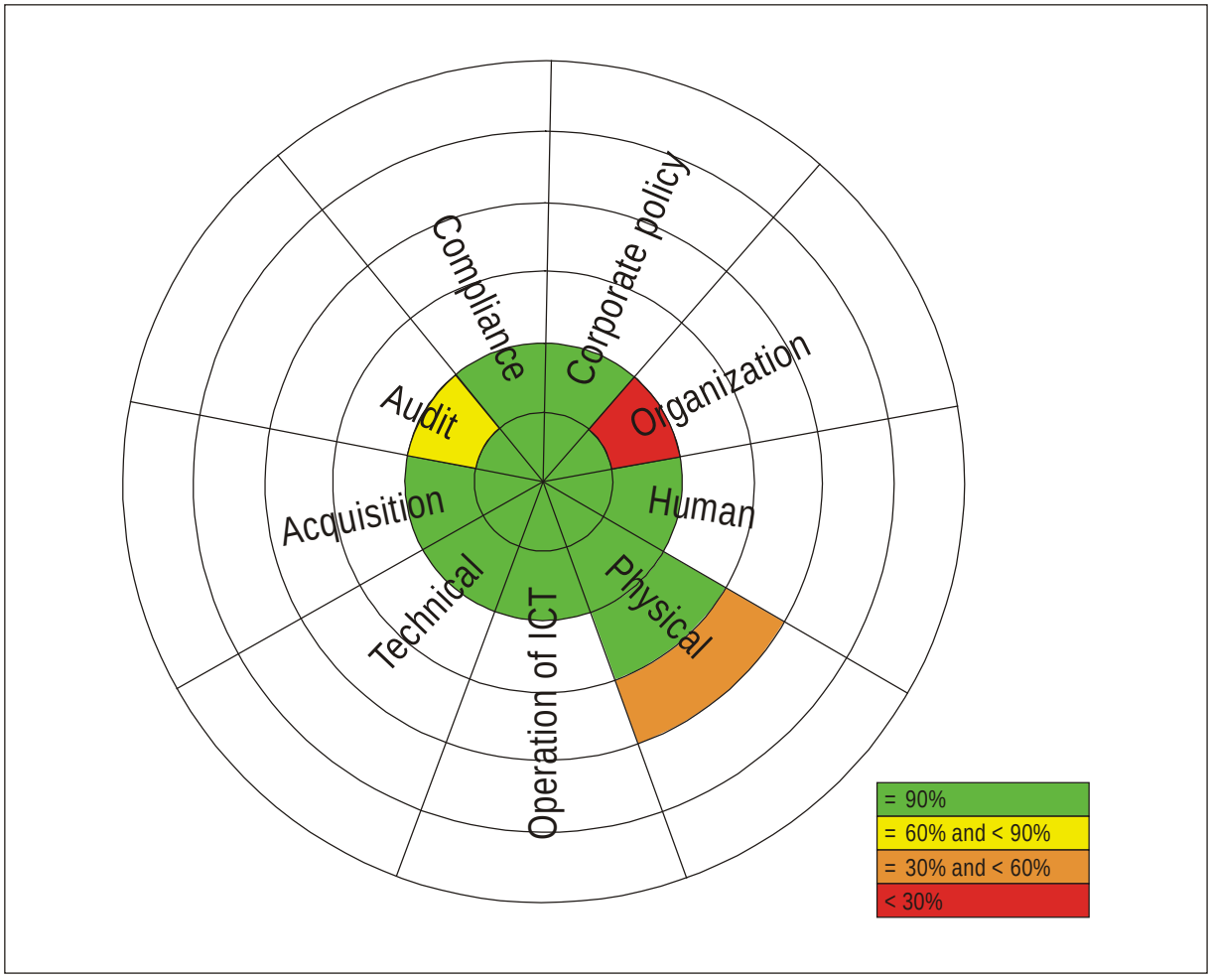


Figure App C-1. Example graphic display of control levels

Table App C-1. Characteristics of level of controls

	Information	*Scope of Protection*	*Isolation of Critical ICT Asset*	*Assumed Threat*
Level 1	Handles sensitive information[1]	Critical information assets	Isolated[2]	Common ubiquitous threats (e.g., hackers and minor criminals)
Level 2	Handles sensitive information	All information assets	Highly connected IT system	Common ubiquitous threats (e.g., hackers and minor criminals)
Level 3	For sensitive operations	Adds medium security controls for identified important assets	Extent of exposure to a higher threat environment is small in comparison to the total ICT systems within the organization.	More sophisticated and better resourced adversaries (e.g., those engaged in serious or organized crime including certain terrorist organizations)
Level 4	For sensitive operations	Medium security for the entire organization[3]	Highly integrated information infrastructure	More sophisticated and better resourced adversaries (e.g., those engaged in serious or organized crime including certain terrorist organizations)
Level 5	Information assets are of high value to itself and to the potential attackers	High-level controls usually specific to the risks and assets	Relatively isolated	Most capable adversaries normally associated with hostile governments (e.g., actual threats from governments, government-sponsored terrorism or industrial espionage, and some very capable criminal organizations)
Level 6	Information assets are of high value to itself and to the potential attackers	Harden whole organization with high-level controls	Widespread assets and cannot be sufficiently isolated	Most capable adversaries normally associated with hostile governments (e.g., actual threats from governments, government-sponsored terrorism or industrial espionage, and some very capable criminal organizations)

1. "Sensitive information" is defined by organization in its risk assessment and includes that covered by legal requirements such as data protection.
2. Isolation must be proven by examination, not merely asserted. Organizations are typically unaware of "back doors" left by installation; provided, even required, for vendor support; or installed by personnel for convenience. Systems should be assumed to have external connections until proven otherwise.
3. If there were a security architect, security controls would be allocated to systems and protection between systems in a more efficient and effective security management.

Table App C-2. Organizational direction and policy

Level	*Control Requirements*
Level 1	1.1. An ICT security policy document covering the critical systems shall be approved by management, and published and communicated to all employees and relevant external parties with responsibilities directly relevant to these systems. *Note.— At Level 1 most controls are restricted in scope to critical systems and the wording is amended accordingly. The restriction is removed at Level 2.*
Level 2	1.2. The ICT security policy document covers all systems and is communicated to all employees and relevant external parties. There are also specific system security policy documents. 1.3. The ICT security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.
Level 3	1.4. Management has adopted a systematic risk management methodology and uses it for assessing and managing ICT security risks.
Level 4	No additional controls at this level.
Level 5	No additional controls at this level.
Level 6	No additional controls at this level.

Table App C-3. Organization culture and management

Level	*Control Requirements*
Level 1	2.1 Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of ICT security responsibilities. *Note.— This is core, without top management commitment the whole edifice is built on sand.* 2.2 All ICT security responsibilities shall be clearly defined. 2.3 A management authorization process for new information processing facilities involving critical functions shall be defined and implemented. 2.4 The organization's approach to managing ICT security and its implementation (i.e., control objectives, controls, policies, processes, and procedures for ICT security) shall be reviewed internally when significant changes to the security implementation occur in operations critical areas. 2.5 The risks to the organization's information and information processing facilities from operations processes involving external parties shall be identified and appropriate controls implemented before granting access.

Level	*Control Requirements*
	2.6 All ICT assets shall be clearly identified and an inventory of all important assets drawn up and maintained. All information and ICT assets shall be owned by a designated part of the organization. Rules for the acceptable use of information and ICT assets associated with information processing facilities shall be identified, documented, and implemented. *Note.— ICT asset identification is essential for risk management. Also it is impossible to enforce security or build a security culture without a clear appreciation of acceptable behaviour.* 2.7 ICT security events concerning critical systems shall be reported through appropriate management channels as quickly as possible. 2.8 Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to ICT security incidents. 2.9 A managed process shall be developed and maintained for operations continuity throughout the organization that addresses the ICT security requirements needed for the organization's operations continuity. *Note.— Operations continuity is closely linked to security. The twin objectives are to prevent loss of operations-critical capability and to ensure that contingency or emergency operations do not compromise other security goals unacceptably.* 2.10 Events that can cause interruptions to critical operations processes shall be identified, along with the probability and impact of such interruptions and their consequences for ICT security.
Level 2	2.11 Management has created a framework and an awareness program fostering a positive control environment throughout the entire organization. This addresses the integrity, ethical values and competence of the people, management philosophy, operating style and accountability. Specific attention is given to ICT aspects, including security and operations continuity planning. Management plans for appropriate resources for policy implementation and for ensuring compliance, so that they are built into and are an integral part of operations. Management also monitors the timeliness of the policy implementation. Although training generally comes under the HR category, we include this control here because of its importance as a leadership tool in creating an appropriate culture of security. 2.12 A management authorization process for all new information processing facilities, based on risk assessment, shall be defined and implemented. 2.13 All operations processes which can support ICT security (e.g., procurement, co-operation with other organizations) shall be organized to provide that support in a secure manner. 2.14 The scope of 3, 7 and 10 is extended to all systems and the whole organization.
Level 3	2.15 There is a formal ICT security organization which supports operations. Once the security requirement exceeds the basic levels dedicated assistance is needed. 2.16 ICT security activities shall be coordinated by representatives from different parts of the organization with relevant roles and job functions. 2.17 The security reviews as in 2.4 are independent.

Level	*Control Requirements*
	2.18 All identified security requirements shall be addressed before giving customers access to the organization's information or assets. 2.19 Information shall be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization (e.g., using EC 2096/2005). An appropriate set of procedures for information labelling and handling shall be developed in accordance with this classification scheme. 2.20 All employees, contractors and third party users of ICT systems and services shall be required to note and report any observed or suspected security weaknesses or malfunctions in systems or services. 2.21 There shall be mechanisms in place to enable the types, volumes, and costs of ICT security incidents to be quantified and monitored. Where a follow-up action against a person or organization after an ICT security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). *Note.— This includes monitoring for acceptable usage, as well as intrusion detection, etc.* 2.22 Plans shall be developed and implemented to maintain or restore operations of critical operations systems and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical operations processes. Operations continuity plans shall be tested and updated regularly to ensure that they are up to date and effective. 2.23 The risk management methodology of 1.4 is at the heart of the decision process for managing ICT security, from selection of controls, systems acquisition and accreditation to operational procedures. Personnel from operational units play an active part in the risk management process alongside their technical colleagues and management.
Level 4	2.24 Requirements for confidentiality or nondisclosure agreements reflecting the organization's needs for the protection of information shall be identified and regularly reviewed 2.25 Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements. 2.26 A single framework of operations continuity plans shall be maintained to ensure all plans are consistent, to consistently address ICT security requirements, and to identify priorities for testing and maintenance.
Level 5	2.27 Appropriate contacts with special interest groups or other specialist security forums.
Level 6	No additional controls at this level.

Table App C-4. Human resources security

Level	*Control Requirements*	
Level 1	3.1	Security roles and responsibilities of employees, contractors and third party users involved with critical systems shall be defined and documented in accordance with the organization's ICT security policy. Management shall require such employees etc. to apply ICT security measures in accordance with established policies and procedures of the organization.
	3.2	References are required on all candidates for employment in sensitive areas or with specific ICT security responsibilities.
	3.3	As part of their contractual obligation, employees, contractors and third party users with access to critical ICT systems shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for ICT security.
	3.4	All security-sensitive employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.
	3.5	Responsibilities for performing employment termination or change of employment security functions shall be clearly defined and assigned.
	3.6	All employees, contractors and third party users shall return all of the organization's ICT assets in their possession and their access rights are removed upon termination of their employment, contract or agreement.
Level 2	3.7	The scope of 3.1, 3.2, 3.3 and 3.4 extends to all employees and, where relevant, contractors and third party users.
	3.8	Breaches of security by employees are investigated and noted.
	3.9	Employees are given an opportunity to give feedback to the organization on ICT security matters when leaving employment.
Level 3	3.10	Basic verification checks on all candidates for employment, contractors, and third party users with access to critical ICT systems or with specific security responsibilities.
	3.11	There shall be a formal disciplinary process for employees in sensitive areas who have committed a security breach.
	3.12	Employees working in sensitive areas or with specific security responsibilities are required to complete a security report when leaving employment.

Level	*Control Requirements*	
Level 4	3.13	The scope of 3.10 and 3.11 extends to all employees and, where relevant, contractors and third party users.
	3.14	ICT security is an explicit responsibility of line management and security attitudes and performance are reported in the appraisal system.
	3.15	All employees should have a security interview when leaving employment.
Level 5	3.16	Background verification checks beyond the basic level are carried for those as in 3.10.
	3.17	Managers have formal responsibility for ICT security performance within their area of responsibility.
Level 6	3.18	The scope of 3.16 extends to all employees and, where relevant, contractors and third party users.

Table App C-5. Physical and environmental security

Level	*Control Requirements*	
Level 1	4.1	Security perimeters (barriers such as walls, card-controlled entry gates or manned reception desks, escorting of visitors) shall be used to protect ICT areas that contain information and information processing facilities of a critical nature.
	4.2	Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied for operations-critical information processing facilities.
	4.3	Equipment used for critical ICT functions shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. It is also protected from power failures and other disruptions caused by failures in supporting utilities. Consideration shall be given to provision of uninterruptible power supply (UPS).
	4.4	ICT equipment shall be correctly maintained to ensure its continued availability and integrity.
	4.5	Security shall be applied to off-site equipment used for critical functions taking into account the different risks of working outside the organization's premises.
Level 2	4.6	The scope of 4.1 is extended to cover all information and information processing facilities. The scope of 4.2, 4.3 and 4.5 is similarly extended.

Level 3	4.7	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. Physical security for offices, rooms, and facilities where sensitive information is processed or accessed shall be designed and applied. Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from secure information processing facilities to avoid unauthorized access.
	4.8	Power cabling and telecommunications communication (physical and wireless), carrying sensitive or operations-critical data and/or voice or supporting such ICT services shall be protected from damage.
	4.9	All ICT equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.
Level 4	4.10	The scope of 4.7 extends to all information processing facilities and all offices, rooms, and facilities, and 4.8 extends to all telecommunications cabling.
	4.11	ICT equipment, information or software shall not be taken off-site without prior authorization.
Level 5	4.12	Telecommunications cabling carrying critical data or supporting such ICT services shall be protected from interception.
Level 6	4.13	The scope of 4.12 extends to all telecommunications cabling. Advice has been sought from national authorities.

Table App C-6. Operation of ICT systems

Level	*Control Requirements*	
Level 1	5.1	Operating procedures for critical ICT systems shall be documented, maintained, and made available to all users who need them.
	5.2	Changes to critical information processing facilities and ICT systems shall be controlled.
	5.3	It shall be ensured that ICT security controls, service definitions and delivery levels included in any third party service delivery agreement are implemented, operated, and maintained by the third party. The services, reports and records pertaining to critical ICT functions provided by the third party shall be regularly monitored and reviewed, and audits are carried out regularly.
	5.4	Networks that are operations-critical or carry sensitive information shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
	5.5	There shall be procedures in place for the management of removable media. Media shall be disposed of securely and safely when no longer required.
	5.6	Policies and procedures shall be developed and implemented to protect information associated with the interconnection of sensitive operations ICT systems.

Level	*Control Requirements*
	5.7 Formal contracts shall be in place establishing agreement between business partners on communication processes and on standards for transaction message security and data storage. When conducting business on the Internet, policy shall require and management shall enforce adequate controls to ensure compliance with local laws and customs on a world-wide basis. Among these are verification of the authenticity of the counterparty providing electronic instructions or transactions and protection of information involved in electronic information passing over public networks from fraudulent activity, contract dispute, and unauthorized disclosure and modification. 5.8 An access control policy for critical ICT systems shall be established, documented, and reviewed based on operations and security requirements for access. There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all such ICT systems and services. The allocation and use of privileges shall be restricted and controlled. All users of critical ICT systems shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user. Inactive sessions shall shut down after a defined period of inactivity. 5.9 Users shall be required to follow good security practices in the selection and use of passwords and shall ensure that unattended equipment has appropriate protection. 5.10 Users of critical ICT systems shall only be provided with access to the network services that they have been specifically authorized to use. 5.11 Access to operating systems shall be controlled by a secure log-on procedure. 5.12 Data input to or output from critical ICT applications shall be validated to ensure that input data is correct and appropriate and the processing of stored information is correct and appropriate to the circumstances.
Level 2	5.13 The scope of 5.1 and 5.2 extends to all operating procedures and information processing facilities respectively. 5.14 The scope of 5.3 extends to all third party agreements for IT provision. 5.15 The scope of 5.6, 5.8, 5.9, and 5.10 extends to all ICT systems. 5.16 The scope of 5.4 extends to all networks. 5.17 The authentication and integrity of information originated outside the organization, whether received by telephone, voicemail, paper document, fax or email, is to be appropriately checked before potentially critical action is taken. 5.18 Users systematically control the activity of their proper account(s). Also, ICT security mechanisms are in place to allow them to oversee normal activity as well as to be alerted to unusual activity in a timely manner. 5.19 Access to ICT and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.

Level	*Control Requirements*
Level 3	5.20 The scope of 5.12 extends to all appropriate applications. 5.21 Management shall ensure that reaccreditation of security (e.g., through "tiger teams") for critical ICT systems is periodically performed to keep up-to-date the formally approved security level and the acceptance of residual risk. 5.22 Duties and areas of responsibility within secure areas shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's ICT assets. 5.23 Development, test and operational facilities shall be separated to reduce the risks of unauthorized access or changes to the operational system. 5.24 Changes to the provision of critical ICT services, including maintaining and improving existing ICT security policies, procedures and controls, shall be managed, taking account of the criticality of operations systems and processes involved and reassessment of risks. 5.25 The use of resources for critical ICT functions shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance. 5.26 Acceptance criteria based on formal risk analysis for new ICT systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance for critical functions. At Levels 3 and 4 we require more formality in procedures. 5.27 The process for controlling (and disposal of) media as in 5.5 is a formal one. 5.28 Procedures for the handling and storage of sensitive or critical information shall be established to protect this information from unauthorized disclosure or misuse. 5.29 System documentation for critical systems should be protected against unauthorized access. 5.30 Formal exchange policies, procedures, and controls shall be in place to protect the exchange of sensitive information through the use of all types of communication facilities. Agreements shall be established for the exchange of sensitive information and software between the organization and external parties; and Media containing such information shall be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries. 5.31 The allocation of passwords for access to critical ICT systems shall be controlled and management reviews users' access rights through a formal process. 5.32 A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted in secure areas. *Note.— A clear screen (or desk) policy is one where users leave nothing on their screen (or desk) when they are absent. Often clear screen policies are enforced for absences of a few minutes, whereas clear desks may only be required overnight, provided the room is secured for temporary absences during the day*.

Level	*Control Requirements*
	5.33 A policy, operational plans and procedures shall be developed and implemented for teleworking activities. 5.34 A specific risk analysis is undertaken before authorizing the use of mobile code on a critical system. The operational case has to be very strong for such authorization to be considered. (This extends the control in ISO 27001.)
Level 4	5.35 The scope of 5.22 and 5.32 extends throughout the organization. 5.36 The scope of 5.24 extends to all third party provided ICT services. 5.37 The scope of 5.21, 5.25 and 5.26 extends to all information processing systems. 5.38 Management obtains independent certification/accreditation of security and internal controls prior to implementing critical new ICT services or using ICT service providers and re-certification/reaccreditation of these services on a routine cycle after implementation. 5.39 The scope of 5.28 extends to all information being exchanged with outside parties. 5.40 The scope of 5.29 extends to all systems. 5.41 The formal process of 5.31 extends to all systems.
Level 5	5.42 In order to minimize the risks and the possibilities of misuse in a network in operation, operational areas dealing with critical operations issues and information are kept separate, logically or physically. As well, development facilities are separated from operational facilities. 5.43 Areas subject to a clear desk/screen policy (see 5.32) are routinely checked out of hours. 5.44 Remote access to a critical system is only authorized in exceptional circumstances following a specific risk analysis. 5.45 Restrictions on connection times shall be used to provide additional security for high-risk applications. 5.46 Remote work on sensitive data should only take place from appropriately secure sites.
Level 6	5.47 The scope of 5.43 and 5.45 extends to all systems. 5.48 Teleworking should only take place from appropriately secure sites.

Table C-7. Technical mechanism and infrastructure

Level	*Control Requirements*
Level 1	6.1 Detection, prevention, and recovery controls to protect against malicious code in all systems and appropriate user awareness procedures shall be implemented. 6.2 Where the use of mobile code is authorized in a critical ICT system, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code should be prevented from executing. Examples of mobile code include Java applets and ActiveX that may otherwise be downloaded and executed without a user's knowledge.[4] 6.3 Appropriate authentication methods shall be used to control access to critical ICT systems by remote users. 6.4 A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities. Mobile computing and communication range from the use of laptop computers in hotel rooms or wireless network access within the organization, to bespoke facilities such as mobile command centers.
Level 2	6.5 The scope of 6.2 and 6.3 extends to all systems. 6.6 There is an appropriate network configuration, as is essential for its reliable functioning. This includes a standardized approach for the configuration of servers throughout the organization, and good documentation. Furthermore, servers used for special purposes are only used for these purposes (e.g., no other tasks should run on a firewall), and sufficient protection from failure is in place. 6.7 Information involved in on-line transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay (trusted path), and the integrity of information being made available on a publicly available system should be protected to prevent unauthorized modification. 6.8 Routing controls such as screened subnets shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the operations applications.

4. Restriction to CSC systems (as is normal for Level 1) is not recommended for 6.1 because of the risk of spread of malicious code between systems. Commercial anti-virus products (properly updated), good patch-management, appropriate media control and high penetration of awareness should be adequate for the basic levels.

Level	*Control Requirements*
Level 3	6.9 There shall be mechanisms in place designed to prevent opportunities for information leakage from sensitive systems. 6.10 For critical ICT systems the mechanisms used to implement 6.1 and 2 are strengthened. Examples include the use of white lists to control executable code, regular checks and specific awareness training for all users. The defenses should be tested regularly. 6.11 Security features, service levels, and management requirements of all critical network services shall be identified and included in any network services agreement, whether these services are provided in house or outsourced. 6.12 Physical and logical access to diagnostic and configuration ports on critical ICT systems shall be controlled. Automatic equipment identification shall be considered (and adopted where appropriate) as a means to authenticate connections to critical ICT systems from specific locations and equipment. 6.13 Systems for managing passwords for critical ICT systems shall be interactive and shall ensure quality passwords. 6.14 The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled on critical systems. 6.15 In any teleworking environment involving critical ICT systems, there are mechanisms to detect attempts to gain entry to systems or networks and successful unauthorized entry so that the organization can respond in an appropriate and effective manner. 6.16 Validation checks shall be incorporated into critical applications to detect any corruption of information through processing errors or deliberate acts. 6.17 Requirements for ensuring authenticity and protecting message integrity in critical applications shall be identified, and appropriate controls identified and implemented. 6.18 A policy on the use of cryptographic controls for protection of information shall be developed and implemented. 6.19 Key management shall be in place to support the organization's use of cryptographic techniques.
Level 4	6.20 The scope of 6.10, 6.12, 6.13, 6.14, and 6.15 extends to all systems. 6.21 The scope of 6.11 extends to all network services. 6.22 Information involved in electronic messaging shall be appropriately protected. 6.23 The scope of 6.16 and 16.17 and extends to all appropriate applications. 6.24 There is an appropriate organization-wide ID infrastructure underpinning authentication and access control decisions.

Level	*Control Requirements*	
Level 5	6.25	Strong routing controls shall be implemented for networks connected to sensitive systems to ensure that computer connections and information flows do not breach the access control policy of the operations applications. Real isolation from untrusted paths is required. Sensitive systems shall have a dedicated (isolated) computing environment.
Level 6	6.26	The scope of 6.25 extends to all systems.

Table C-8. Acquisition, development and maintenance

Level	*Control Requirements*	
Level 1	7.1	Statements of operations requirements for new ICT systems, or enhancements to existing ICT systems for critical functions shall specify the requirements for security controls.
	7.2	There shall be procedures in place to control the installation of software on operational systems, with critical functions.
	7.3	When operating systems are changed, operations critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
	7.4	Security patches should be obtained and implemented in a timely manner on critical systems.
	7.5	Back-up copies of critical information and software shall be taken and tested regularly in accordance with the agreed backup policy.
Level 2	7.6	The scope of 7.1, 7.2, 7.3 and 7.4 extends to all ICT systems.
	7.7	Management has implemented procedures to ensure that operations and user management formally accept the test results and the level of security for ICT systems, along with the remaining residual risk. These procedures reflect the agreed upon roles and responsibilities of end user, system development, network management and system operations personnel, taking into account segregation, supervision and control issues.
	7.8	ICT management has ensured that maintenance personnel have specific assignments and that their work is properly monitored. In addition, their system access rights are controlled to avoid risks of unauthorized access to automated systems.
	7.9	The scope of 7.5 extends to all information and software.

Level	*Control Requirements*
Level 3	7.10 ICT security underpinned by risk management is integrated within the organization's project management and quality control methodologies. 7.11 Test data for critical ICT functions is selected carefully, and protected and controlled and access to program source code shall be restricted. This requirement is difficult to interpret because an extreme reading would prohibit the use of both proprietary operating systems and open source software. The essentials are that: • Software is carefully and appropriately tested; • The source of any software is considered to be sufficiently trustworthy for the specific application; and that; and • Detailed system configuration information should be protected. 7.12 The implementation of changes to critical ICT systems is controlled by the use of formal change control procedures that include a security risk assessment. 7.13 Modifications to software packages on critical ICT systems is discouraged, limited to necessary changes, and all changes shall be strictly controlled. 7.14 Timely information about technical vulnerabilities of ICT systems in use shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk. 7.15 Off-site storage of critical back-up media, documentation and other ICT resources is established to support recovery and operations continuity plans. Operations process owners and ICT function personnel are involved in determining what back-up resources need to be stored off-site. The off-site storage facility is environmentally appropriate to the media and other resources stored and has a level of security commensurate with that needed to protect the back-up resources from unauthorized access, theft or damage. ICT management shall ensure that off-site arrangements are periodically assessed, at least annually, for content, environmental protection and security.
Level 4	7.16 The scope of 7.11 extends to all application and system programs. 7.17 The scope of 7.12 extends to all systems. 7.18 Modifications to software packages on all ICT systems shall be limited to necessary changes, and all changes shall be strictly controlled.
Level 5	7.19 Outsourced software development for critical ICT systems shall be supervised and monitored by the organization.
Level 6	7.20 The scope of 7.19 extends to all systems.

Table C-9. Monitoring and audit

Level	*Control Requirements*	
Level 1	8.1	For all critical ICT systems, audit logs recording user activities, exceptions, and ICT security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.
	8.2	System administrator and system operator activities on critical ICT systems shall be logged.
	8.3	Faults on critical systems shall be logged, analysed, and appropriate action taken.
	8.4	Audit requirements and activities involving checks on critical operational ICT systems shall be carefully planned and agreed to minimize the risk of disruptions to operations processes.
	8.5	Access to ICT systems audit tools used for critical ICT systems shall be protected to prevent any possible misuse or compromise.
Level 2	8.6	The scope of 8.1, 8.2, 8.3, 8.4, and 8.5 extends to all systems.
	8.7	Policies and techniques have been implemented for using, monitoring and evaluating the use of system utilities. Responsibilities for using sensitive software utilities have been clearly defined and understood by developers, and the use of the utilities is monitored and logged.
Level 3	8.8	Procedures for monitoring use of critical information processing facilities shall be established and the results of the monitoring activities reviewed regularly.
	8.9	Logging facilities and log information for critical ICY systems shall be protected against tampering and unauthorized access.
	8.10	Network monitoring shall be used to identify the weaknesses within the existing network configuration. It allows for reconfiguration caused by traffic analysis and helps to identify attackers.
Level 4	8.11	The scope of 8.8 and 8.9 extends to all ICT systems and information processing facilities.
	8.12	Mechanisms designed to detect attempts to gain entry to systems or networks and successful unauthorized entry are in place so that the organization can respond in an appropriate and effective manner.
Level 5	8.13	The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an accurate time source.
Level 6	No additional controls at this level.	

Table C-10. Compliance

Level	*Control Requirements*
Level 1	9.1 All relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each ICT system and the organization as a whole. 9.2 Important records are protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and operations requirements. 9.3 Data protection and privacy are ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. 9.4 Managers shall ensure that all ICT security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.
Level 2	9.5 Appropriate procedures are implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products. 9.6 There are prominent rules against using information processing facilities for unauthorized purposes, which all users are expected to obey, reinforced by a disciplinary process. ISO 27001 15.1.5 just says 'Users shall be deterred from...'
Level 3	9.7 Cryptographic controls are used in compliance with all relevant agreements, laws, and regulations. 9.8 The rules as in 9.6 are reinforced by technical and physical checks and a strict disciplinary process. 9.9 ICT systems are regularly checked for compliance with security implementation standards.
Level 4	No additional controls at this level.
Level 5	No additional controls at this level.
Level 6	No additional controls at this level.

Appendix D

NATIONAL AND REGIONAL EXAMPLES OF PROVISION FOR ATM SECURITY SERVICES

This appendix provides information on procedures and practices currently in use for States and Civil Aviation Authorities to consider when provisioning ATM security services of ATSP's. Three sections of the appendix review EUROCONTROL, United Kingdom, and United States ATM security services for inflight incident management and crisis management coordination.

1. IN-FLIGHT SECURITY INCIDENT MANAGEMENT FRAMEWORK IN EUROPE

1.1 EUROCONTROL and NATO have created an operational concept for in-flight security incidents in Europe. This concept coordinates actions of NATO and EUROCONTROL during in-flight security events. This appendix presents the concept of operations.

Introduction

1.2 The tragic events on September 11, 2001 drastically changed the way in-flight security incidents are managed as the world witnessed an unprecedented dimension of terrorism; civil aircraft being used as weapons of mass destruction. In Europe, the new threat was termed Renegade.[1] Since then, national security authorities are more reactive to any indication that could lead to a security concern, i.e., COMLOSS with the aircraft, or transponder switch off or wrong setting. As an example, in most European countries the number of interceptions due to COMLOSS at least doubled after September 11.

European response

1.3 In light of the new threat, Renegade, national response procedures to deal with in-flight security incidents were reviewed. In many cases bilateral agreements were set up to better coordinate cross-border incidents. However, the international dimension of in-flight security incidents requires harmonization at the European level. As an example, Figure App D-1 represents the September 11 aircraft tracks mapped onto a central European scenario and shows that three or four States are affected by an incident that takes place in a short timeframe.

1.4 To address the international dimension of the Renegade issue, EUROCONTROL and NATO created the NATO EUROCONTROL Air Traffic Management (ATM) Security Coordinating Group (NEASCOG) with the mission to ensure the necessary close co-ordination and development of all related security activities with the aim that the member nations of each organization reach converging views.

1. A situation where a civil aircraft is used as weapon to perpetrate a terrorist attack is usually referred to as a Renegade.

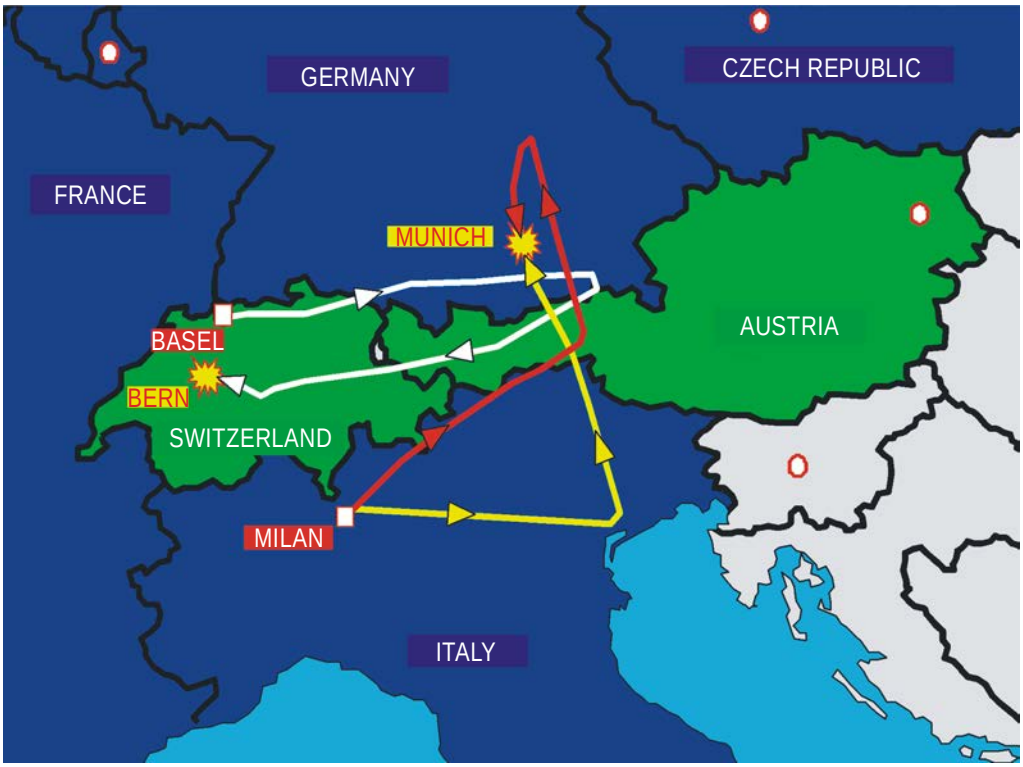


Figure App D-1. September 11 aircraft tracks mapping on Central European scenario

1.5 In this regard the NEASCOG promotes, develops and supports effective pan-European security measures; that is:

a) create a European Regional focal point for ATM information involving civil and military interests; and

b) give priority to the validation of a high capacity air-ground communications, capability for the transmission of encrypted cockpit voice, flight data and on-board video information.

Explaining the problem

1.6 In-flight security incidents are time critical events which require strong coordination among different actors and the gathering and validation of nearly real time information for decision-making support.

1.7 The main aspects to manage during a security incident are:

a) optimizing awareness: identification of suspicious aircraft, incident notification, information dissemination, maintaining awareness;

b) information requirements: relevant information needed to manage and resolve an incident;

c) time factor: required information must reach the appropriate recipient on time to be able to provide adequate response; and

d) technology support: automation and encryption facilitate information exchange, reduce delays and guarantee confidentiality.

1.8 Information requirements for in-flight security incidents have been gathered from national authorities. Relevant information items are:

a) determine if behaviour is suspicious. Several criteria for suspicious behaviour have been identified, but the list is not exhaustive. Training, security awareness and best judgment of pilots and controllers are therefore a key factor;

b) gather information about the event. Information about situation on board is essential. The pilot-in-command (PIC) is the key actor, and measures to support the PIC must be implemented according to pre-defined scenarios when possible. However, a key issue is to make sure that the PIC is legitimate. Other information about the flight is also important;

1) type of aircraft;

2) nationality;

3) operator;

4) passengers on board, nationality;

5) VIPs; and

6) children;

c) assess the risk. Risk assessment should include consideration of the real threat posed by the aircraft based on factors such as; endurance, objectives at range, aircraft behaviour (i.e., deep descent), confirmation of legitimate PIC and pilots' intention.

Providing solutions: the framework

1.9 The NEASCOG airspace security incident management (ASSIM) high level concept provides a framework to deal with in-flight security incidents. The objective of the concept is to support the decision making process by providing the national authorities responsible for airspace security[2] with real time reliable information about airspace security incidents.

1.10 Other actors considered in the ASSIM high level concept are: national air defence centres, adjacent air defence centres, civil ATC, airline operations centres and the aircraft (See Figure App D-2).

1.11 One of the domains that must be considered within the ASSIM concept is the technical support (ASSIM tool) enabling secure and real time dissemination of information.

2. Airspace Security: safeguarding of the airspace of responsibility from unauthorized use, intrusion, illegal activities or any other violation. This involves managing the airspace to prevent, detect and resolve where possible airborne threats.

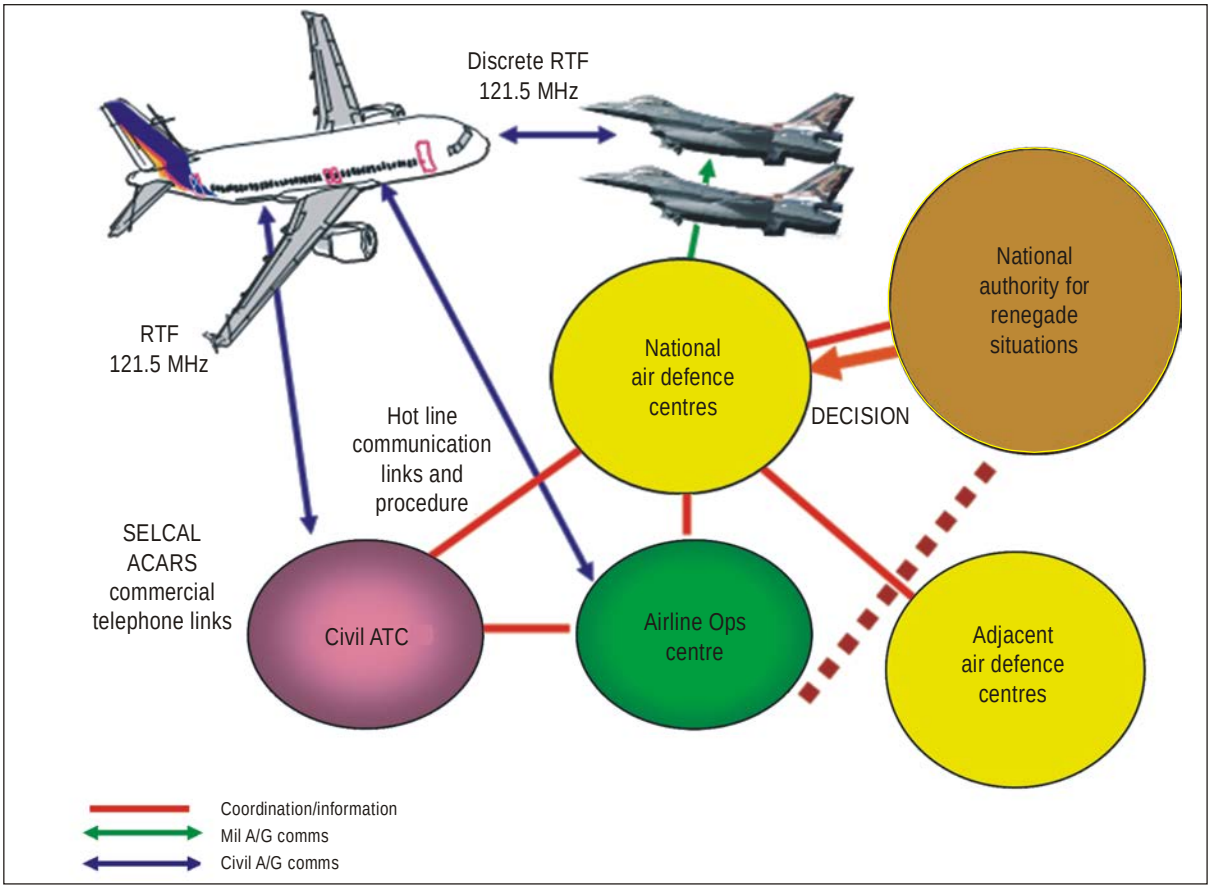


Figure App D-2. Airspace security incident management high level concept

Technical support (ASSIM supporting tool)

1.12 A fundamental aspect of ASSIM is the collection and timely dissemination of the required information. The ASSIM concept considers the National Governmental Authorities (NGA) as the end user. The rest of the actors should play a role to support the NGA and facilitate the decision making process.

1.13 An ASSIM tool should therefore be tailored taking into account the NGA needs. An automated ASSIM tool will clearly benefit the national decision making process by gathering and disseminating in real time secured (i.e., encrypted) information. Pre-defined sets of information items must be available immediately if an incident escalates to NGA level; only an automated tool can provide for this, especially in a multiple event scenario.

1.14 Commercial off-the-shelf (COTS) products should provide the best option for the ASSIM tool, from a pragmatic and cost-efficiency point of view.

ASSIM supporting tool components

1.15 Taking into consideration information provided in above paragraphs, the two keys aspects for the management of in-flight security incidents are:

a) real-time availability of secured information of the situation on board; and

b) real-time security information sharing, including situation on board

1.16 Technology can support both, the acquisition of airborne information and the sharing of security information through a network. EUROCONTROL and NATO are involved in two pilot projects addressing both aspects, in order to assess feasibility and implementation options.

Airborne information acquisition

1.17 In-flight security can be enhanced by providing real-time encrypted information (voice, data and video) from aircraft to the ground. The information would provide the security authorities with much-improved situation awareness in the event of malicious interference with an aircraft in flight. See Figure App D-3.

1.18 The availability of suitable radio spectrum is critical for all systems that transmit or receive. This means that any new aeronautical system must be accommodated within existing aeronautical spectrum and must be compatible with other systems.

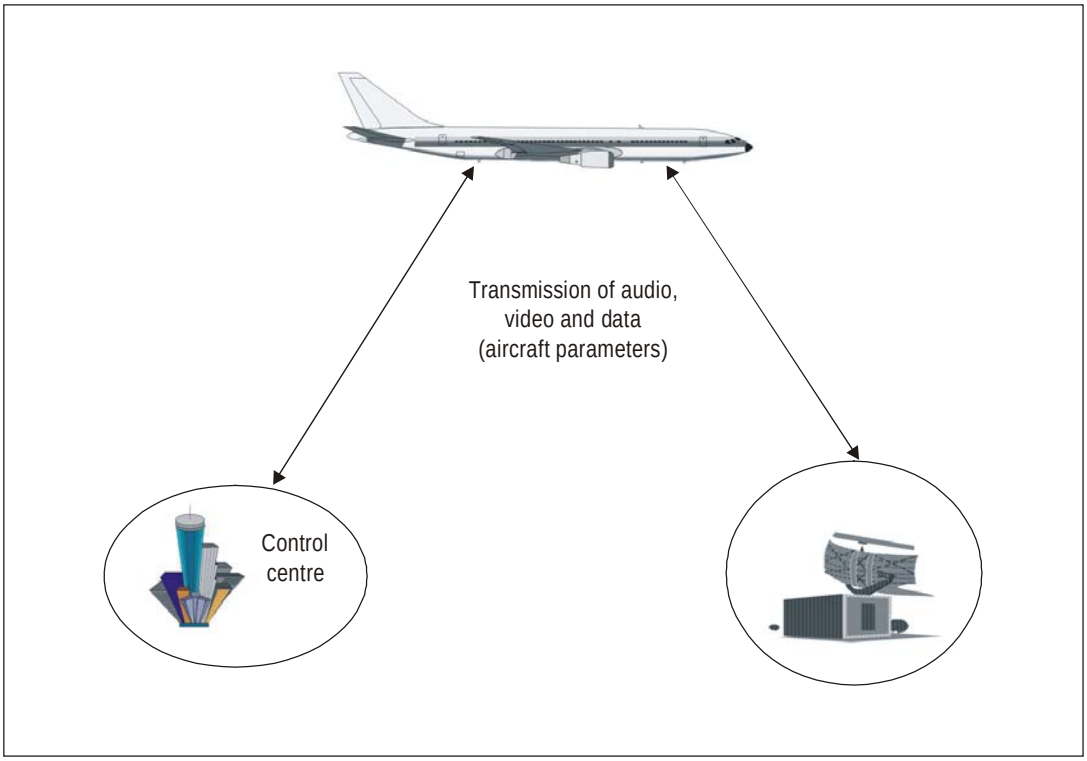


Figure App D-3. Airborne information acquisition

Security information sharing

1.19 Once security information has been acquired, the second step is sharing this information among all actors involved in in-flight incidents. Sharing improves the ability to assess the situation, take the appropriate actions and facilitate and support the decision making process. However, information must be shared in a secure manner to protect privacy and confidentiality.

1.20 The current project relies on the Private Key Infrastructure (PKI) technology, which is more and more widely used in both the civil and military environments (See Figure App D-4). PKI brings a solution for several basic problems of confidence and trust in the electronic world including:

a) identity of a user;

b) authentication, integrity, and non-repudiation through digital signature;

c) privacy and confidentiality through encryption;

d) information cannot be manipulated; and

e) information cannot be disowned.

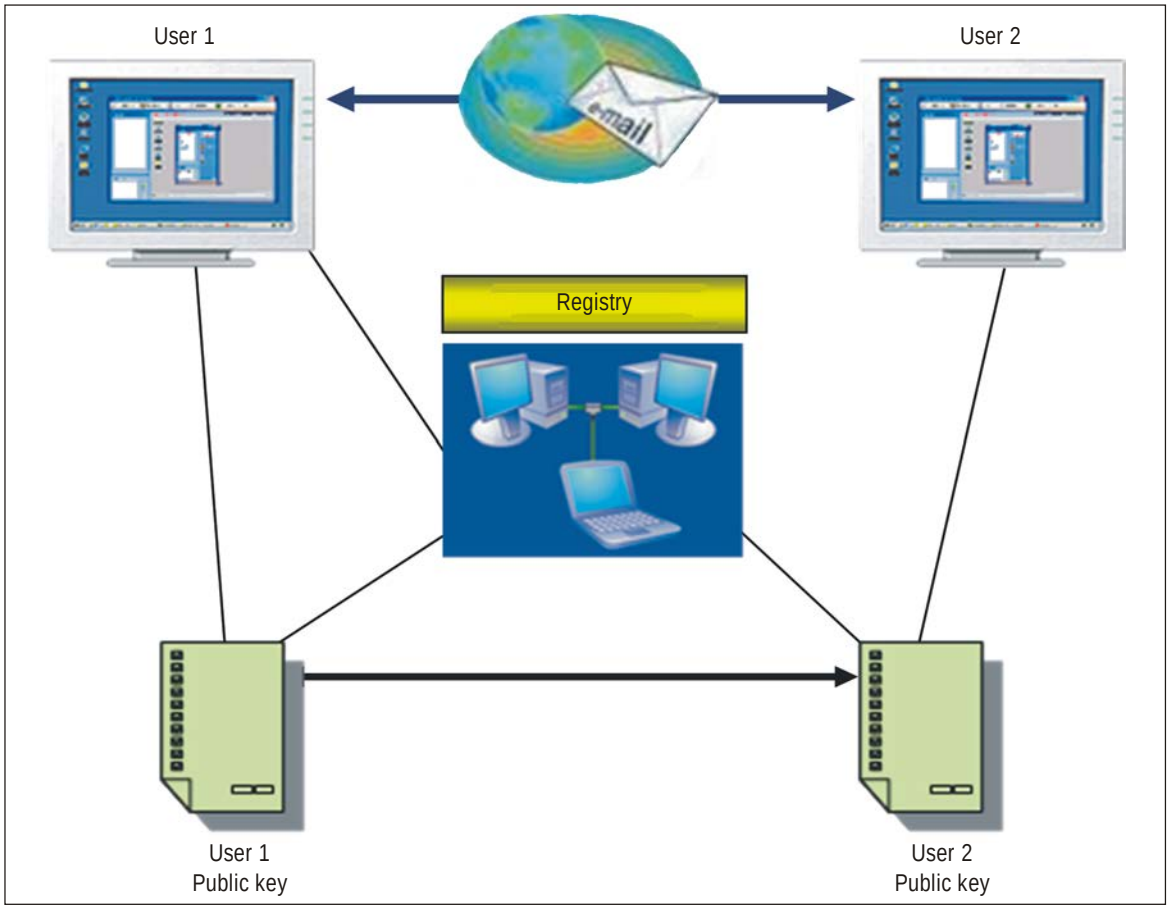


Figure App D-4. Secure email framework

1.21 PKI offers a secure (PKI encryption) environment for the exchange of security related information, and the additional advantage that it may be interfaced with any other IP based security application, providing for compatibility with, for example, the airborne component (paragraph E-2.6.1).

2. IN-FLIGHT SECURITY EVENT PROCEDURES IN THE UNITED KINGDOM

2.1 UK NATS, the United Kingdom's ATSP, has published security procedures for handling in-flight security events such as hijacking, bomb threat, or irregularities such as communications loss or unauthorized change of transponder code. Their procedures are presented here as reference for member states wishing to review other ATSP's procedures.

Introduction

2.2 The following guidance should assist aircraft operators, threat assessors and pilots in understanding of the procedures which will be followed by the appropriate UK authorities when handling airborne security events. The overall objective is to identify, contain and resolve an airborne security situation in an appropriate way and as quickly and safely as possible.

2.3 In the interests of national security both ATC and air defence (AD) agencies monitor UK airspace and its approaches for indications of suspicious activity which may indicate a developing airborne security event, so that suitable action can be taken to deal with the situation. An airborne security event occurs when an aircraft is either subject to an actual or perceived threat, which may take the form of a hijacking, bomb alert or other on-board disruption, or that aircraft is perceived to pose a threat to the UK. In either case the procedures used to determine the actuality, nature and extent of this threat will be similar. The procedures used to deal with each type of threat, however, are likely to be different.

2.4 If an airborne security event is believed to pose a threat to the UK it is likely that the AD Authority (ADA) vested in the National Air Operations Centre (NAOC) RAF High Wycombe) may use Quick Reaction Alert (QRA) aircraft and other assets to gain further information and take necessary action to resolve the situation. The situation is likely to evolve rapidly and therefore timely passage of information and compliance with instructions is key.

2.5 The procedures here described are owned by the UK Government and contain actions for a variety of agencies, principally the Ministry of Defence (MoD), NATS, the Department for Transport (DfT) and the Metropolitan Police Service. These procedures are regularly reviewed and are applicable whether the subject aircraft, regardless of nationality, is inbound, outbound or overflying the UK, and apply to the whole of UK airspace i.e., the London and Scottish FIRs and Upper Information Regions (UIRs) and the Shanwick Oceanic Control Area.

Identification/indication of hijacks and airborne security situations

2.6 Verified Hijack Status. Aircraft subject to hijacking should, where possible, be identified to ATC staff by the flight crew's selection of the Mode 3/A code 7500 on the aircraft transponder and/or declaration on the radio transmitter facility (RTF) frequency.

2.7 Other Security Alert Indicators. There are a range of indicators of suspicious aircraft/pilot activity which could highlight a potential security event to ATC and AD agencies and lead to the initiation of intervention procedures. These indicators include but are not limited to the following:

a) no cleared flight profile, i.e., infringement of airspace;

b) unauthorized deviation from cleared flight profile in the horizontal or vertical plane;

c) refusal or inability to comply with ATC instructions, including vectoring, without good reason;

d) loss of RTF contact, particularly associated with flight profile deviation;

e) unauthorized SSR code changes or extended use of IDENT;

f) use of non-standard phraseology by the crew or other covert attempts to highlight the situation (marked change in voice characteristics, etc.);

g) notification of a threat or incident from official or non-official sources;

h) open RTF transmission from the cockpit;

i) non-ATC related RTF transmission (e.g., political statement); and

j) specific/non-specific threat passed via third party (e.g., police/public).

2.8 The last three items, above, may mean that the identity of the aircraft is unknown until other factors become apparent. Individual events may not, in themselves, constitute suspicious aircraft or pilot activity. However, a combination of such events may be considered as an unusual event and then the appropriate alerting action will be undertaken by ATC.

Pilot-in-charge/aircraft operator responsibilities

2.9 Where information exists indicating an actual or perceived security threat to an aircraft, this information should be communicated to the handling ATC unit immediately by the pilot in charge or to the UK civil security authorities by the aircraft operator as appropriate. A trained airline threat assessor should evaluate the threat and inform cascading findings/codings to the UK civil security authorities as soon as possible. Information regarding the integrity of the flight deck should be provided to ATC in a timely manner. This will ensure that the situation is handled in the most appropriate manner by the UK state defence agencies.

2.10 Appropriate use of RTF phraseology and special purpose Secondary Surveillance Radar (SSR) Mode 3/A codes is essential. If there is an actual security threat, the pilot in charge should not use either PAN or MAYDAY prefixed calls in isolation to communicate the threat to ATC. Details of the security threat must be passed in the same transmission. Where no security threat to the aircraft is perceived by the pilot-in-charge, appropriate use of either PAN (Possible Assistance Needed–no imminent danger to life) or MAYDAY (Distress call - imminent danger to life) should be applied if the pilot in charge requires some form of priority ATC handling to the destination or a diversion airfield.

2.11 Aircrews should be strongly advised to monitor the emergency frequency 121.5 MHz at all times. Routine monitoring of 121.5 significantly increases chances of hearing transmissions from ATC attempting to re-establish contact with the aircraft. Also, military aircraft simulcast on 121.5 in addition to standard ATC frequencies. Aircrews who, for whatever reason, find themselves without the correct frequency are also advised to request assistance from ATC using 121.5 MHz.

2.12 The combination of correct RTF calls and use of Mode A codes will assist ATC to take action appropriate to the situation.

Communications

2.13 ATC. As soon as notification of an event is received, the handling ATC unit will pass the details to the ATC operations supervisor at a parent air traffic area control centre (ACC). It is then the responsibility of that supervisor to notify the UK military defence agencies, via the military ATC organization. The UK military ADA will subsequently notify appropriate UK Government agencies including civil and law enforcement organizations.

2.14 The Police:

a) contribute to the intelligence picture and assist in the bomb threat assessment;

b) act as a single point of contact (SPOC) for the passing of real time information between the UK ADA and the police force responsible for the receiving airport;

c) deploy an effective and flexible police response that is commensurate with the threat and/or incident; and

d) investigate crime.

2.15 Law enforcement operates a Reserve room which acts as their duty office to take calls and provide the UK ADA with any intelligence that the police are aware of in respect of an airborne security incident.

2.16 The Reserve room also acts as a SPOC for police forces receiving mobile phone calls from passengers or crew aboard the Renegade aircraft or from ground based relatives of passengers relaying such information. These calls, which may contain vital intelligence or information, are then relayed to the UK ADA to assist in the assessment of the developing incident.

2.17 As the event progresses, the civil ATC, military ATC and UK ADA will coordinate their actions and, where and when the relevant authority makes decisions, will implement any operational directives. The UK ADA will continue to liaise with civil and law enforcement agencies, both of whom will continue to provide intelligence and information as it becomes available, to aid the ADA's decision-making process.

2.18 In the event specific information is required or must be communicated, the civil security agencies may contact aircraft operators via operations centres and/or key personnel (e.g., threat assessors). Such channels may be used in attempting to establish the security and integrity of the flight deck and/or the nature and degree of the threat posed to or by an aircraft. This channel of communication is vital in determining the nature and extent of the threat.

2.19 It is, therefore, essential that the aircraft operator provide civil security agencies with a 24/7 contact number for their operations centre so that staff can communicate immediately with (a) the airline when seeking to advise of lost communications and requesting associated actions and (b) a trained threat assessor who can assist UK Government agencies in responding proportionately and in a timely fashion to the situation as it unfolds. The lack of a trained threat assessor and/or operations centre point of contact severely limits an airline's ability to participate in, and contribute to, what can be a dynamic and rapidly changing decision-making process.

2.20 Airline operations centres and threat assessors who may be required to pass/receive timely information to assist in the effective handling of a crisis situation should keep a ready list of telephone and contact information for civil security agencies on hand.

UK Air Defence Authority (and associated agencies) Actions

2.21 When notified of a potential airborne incident or threat, the UK ADA determines the initial actions to be taken to ensure the security of UK airspace. Prior to the official declaration of a security incident, the UK ADA may elect to take certain actions to prepare the AD forces. This may include ordering the QRA aircraft to an increased state of readiness and/or launching the QRA aircraft to intercept the aircraft of concern.

2.22 Once advised by the UK ADA, the civil security agency will make every effort to contact the airline operations centre and/or threat assessor. It will also seek to enlist the help of both parties to ensure any response by UK Government agencies is timely, proportionate and effective. It is imperative that airline staff understand that this is a key opportunity to influence and/or educate the decision making process by assisting ATC to regain communications with the aircraft and/or assessing the threat. Failure to be available and/or respond in a timely fashion may limit the options available to the UK Government when considering how best to respond to a fast-moving and dynamic situation.

2.23 If and when the UK ADA initiates the launch of the QRA aircraft, the Military Supervisor at the appropriate Air Traffic Control Centres (ATCCs) will telephone the civil security authorities. The police notification plan will be initiated and link the Military Supervisor to the Force Control Centre of the police force responsible for the airport where the aircraft will land.

2.24 The provision of real time information in this way assists the police ground response and permits continual re-assessment of the threat (in particular by the airline threat assessor) to help the receiving force to deploy the most suitable and proportionate police response. The aim of this response is to preserve life, minimize injury, ensure an early return to normality, and to preserve evidence.

2.25 If the interception of a civil aircraft is ordered by the UK ADA, QRA aircraft will close on the left side of the aircraft while attempting to make contact with the cockpit using VHF radio communications; the military aircraft will simulcast on 121.5 MHz in addition to standard ATC frequencies.

2.26 Voice communications with the cockpit and compliance/ non-compliance with the interception signals assist the UK ADA in determining the intent of those in control of the aircraft. The UK ADA's conclusions will be communicated to the UK Government who will determine what further action should be taken. Such actions could result in the aircraft being diverted into an alternative airport from that which was originally intended.

False Alarms

2.27 False alarms continue to be generated on a regular basis and in the overwhelming majority of cases are caused by:

a) Civil aircraft operated as a controlled flight not maintaining a continuous listening watch on the appropriate radio frequency of, and establishing two-way communication as necessary with, the appropriate ATC unit as they approach or enter UK airspace; or

b) less frequently, bomb threats made against aircraft in-flight where trained airline threat assessors are uncontactable and unable to assist in understanding and coding the nature and severity of the threat.

2.28 NATO colleagues or other ATC agencies will also alert the UK ADA or UK ATC agencies if an aircraft, due to land in or overfly the UK, loses communications for a significant period of time or is faced with a potential threat situation. This can trigger the UK ADA actions described in the sections above. Thus, a loss of communications combined with the aircraft deviating from its flight plan is likely to trigger an immediate launch of the QRA aircraft which may result in the interception and diversion of the aircraft.

2.29 The UK ADA may ask to speak to the commander of any aircraft that triggers an alert (regardless of the actions subsequently taken) once it has landed and further action may be requested through the relevant national authorities if negligence is suspected or no explanation for the loss of communications is offered. Equally, an airline's inability to contribute to the UK Government's understanding of the threat in a timely fashion e.g., by having a trained threat assessor available, may result in the UK Government seeking clarification of an airline's contingency planning capabilities.

2.30 It is accepted that some false alarms will continue to be generated because of operator error and RTF/ground based communication failures. However, it should be borne in mind that they are wasteful of both industry and UK Government resources and have the potential to create danger for those on board, and the UK more generally.

2.31 The UK Government security agency will ask for an explanation of false alarms, particularly for those which result in the launch of QRA aircraft and may request a copy of the internal investigation into such an incident and details of remedial action taken to prevent repetition. Working with British Airlines Pilot Association, a self-reporting form has been developed which pilots involved in COMLOSS incidents can complete to aid with any subsequent investigation. Data elements included in this form are listed in Section D.2.11.1.

Situation Containment

2.32 As part of the reaction to airborne security situations, decisions regarding routing, flight profile and destination (including possible airborne holding) may be taken outside of normal aircraft operator/pilot in charge arrangements. In the event that ATC or the UK ADA feel they have reason to question whether the communication from the flight deck is being made under duress, the aircraft may be instructed to perform specific manoeuvres. It is essential that any such instructions are complied with whether passed by ATC or via standard ICAO intercept procedure signals.

2.33 It should be noted that certain information may be withheld from the pilot in charge during events of this nature, and that some requests by either the aircraft operator or pilot in charge may not be approved by the appropriate UK authorities.

2.34 As part of the response, ATC may be directed to effect airspace clearance measures. These actions may affect other aircraft in the vicinity, including on the ground, and the continuation of existing flight plans may not be permitted. ATC may require diversion to alternate airfields or may withhold clearances. During such times, the flight safety of all aircraft will remain paramount and, as such, aircraft may be issued non-standard ATC clearances.

2.35 The extent, sequence and priority of any temporary airspace /flight restrictions will be at the discretion of the parent ACC supervisor, who will coordinate ACC actions with the relevant civil defence authorities. Priority shall be given to clearing traffic away from all regulated airspace through which the subject aircraft is anticipated to progress. The parent ACC supervisor will act as overall coordinator for the required airspace clearing process, and will use methods such as:

a) cancelling all relevant ATC clearances into airspace likely to be affected by the incident;

b) applying air traffic flow management (ATFM) measures;

c) coordinating with adjacent ATC Units, with particular consideration for the effects on airport operations (e.g., cessation of airborne holding, diversions, etc.) as well as the ability of these units to assist in the off-loading of traffic for affected sectors;

d) temporary re-routing of aircraft to avoid the subject aircraft and progress thereof;

e) cancelling or amending ATC coordination arrangements; and

f) the DfT may order the closure of UK airspace if necessary and all aircraft will be required to comply with the directions given by ATC to achieve this.

Key points for pilots, aircraft operators and threat assessors

2.36 To avoid an incident, pilots, aircraft operators and threat assessors must ensure that:

a) communications with ATC are maintained at all times;

b) civil security agencies have 24/7 contact details for the company operations centre; and

c) a trained threat assessor is available at all times.

2.37 To ensure that any event is handled in the most appropriate manner, the UK Government advises pilots and aircraft operators:

a) to be aware of potential situations such as loss of two-way communications or inadvertent Mode 3/A 7500 code selection that may indicate a potential security alert to ATC and take all necessary precautions to prevent that happening;

b) to communicate clearly to all parties when, in the pilot's opinion, there is an actual or perceived security threat to the aircraft or to the UK;

c) to make contact with the company operations centre at the earliest opportunity to ensure all pertinent information is shared in a timely fashion, speaking with a trained company threat assessor, if necessary;

d) to volunteer information regarding the integrity of the flight deck and the exact nature of the threat/concern to ATC and/or the company operations centre in a timely manner and be clear and concise;

e) to use appropriate RTF phraseology and special purpose SSR Mode 3/A codes; and

f) to comply with government instructions whether given by radio or through visual intercept signals.

Situation Recovery

2.38 Normal ATC operations will not resume until authorized by the relevant authority. Subsequent recovery measures required for the overall ATC system may be managed by the ATSP.

In-flight loss of communications in-flight incident reporting

2.39 Expected communications between ATC and an aircraft in-flight is monitored constantly by UK civil/military ATC. Communications loss is one potential example of suspicious behaviour which may indicate a possible in-flight security incident. The United Kingdom Loss of Communication In-flight Incident Report form enables aircrews to report such incidents so that a) the correct information is recorded as to what exactly happened and b) necessary steps can be taken to reduce the chance of repetition.

Data elements in the form are as follow:

1/ Date
2/ Time UTC
3/ Operator (airline)
4/ Flight Number
5/ Aircraft Call sign (if different)
6/ Departure airport and Destination airport
7/ Squawk/SSR Mode 3/A code
8/ Aircraft Type
9/ Registration/Tail Number
10/ Altitude (at time of incident) FL/feet
11/ Speed (at time of incident): Mach No/Kts
12/ Phase of Flight
13/ Location
14/ Routing
15/ Weather conditions
16/ Channel Frequency (MHz)
17/ Controlled by (ATC sector)
18/ Description of incident
19/ Cause(s): (a) pilot error; (b) ATC hand-over error; (c) technical issues; (d) any other cause, please specify:
20/ Was aircraft to aircraft relay attempted by ATC and result (if attempted)?
21/ Was Ground to aircraft communications on 121.5 MHz attempted?
22/ Were any other communication methods attempted (Aircraft Communications Addressing and Reporting System [ACARS], Satellite, Company frequency etc.)?
23/ Any other pertinent information
24/ Contact details (name, telephone or email address)

3. UNITED STATES DOMESTIC EVENTS NETWORK PROCEDURES

3.1 The United States has developed procedures for coordinating and handling ATM security events in U.S. airspace via the Domestic Events Network, or DEN. An overview of those procedures is included in this section.

3.2 On the morning of September 11, 2001, a conference call was established between various Federal Aviation Administration (FAA) ATC facilities, the FAA Air Traffic Control System Command Centre (ATCSCC), and Northeast Air Defence Sector (NEADS) to coordinate information concerning the hijacked aircraft. That original conference was initiated to coordinate National Airspace System (NAS) security and evolved into what is now referred to as the United States DEN. It is now the primary network for ATM Security coordination in the United States.

3.3 The DEN is a 24/7 interagency unclassified telephonic conference, operated by FAA System Operations Security, dedicated to real-time coordination of security related events in the United States ATM system. Information is shared via the DEN so that all relevant agencies at the federal, State, tribal, and local levels can come together jointly to analyse possible security incidents and form a collaborative interagency response on how to manage the events.

3.4 The FAA was created in 1958 to provide a centralized focus for aviation in the United States. The Homeland Security Act of 2002, the Aviation and Transportation Security Act of 2001, and the formation of the Department of Homeland Security (DHS) and the Transportation Security Administration (TSA) did not alter the FAA's status. The FAA continues to be the sole authority for airspace management, air traffic regulatory authority, and use of airspace. The TSA works closely with, consults and coordinates with the FAA as appropriate on all issues concerning aviation security.

3.5 In circumstances that potentially affect national defence, it is the FAA Administrator — in consultation with the Secretary of Defence — who decides to establish areas in the airspace that are necessary for national defence. Statutory provision explicitly provides for the transfer of a duty, power, activity or facility of the FAA to the military in the event of war. No other such provision exists in regard to the transfer of any duty, power, activity or facility from the FAA to any other government agency or entity.

3.6 Use of the DEN enables acknowledgement and preservation of the respective roles and expertize of the Department of Defence (DOD), TSA, FAA, and law enforcement agencies. The DEN enables coordinated actions and activities that provide maximum effectiveness in the provision of ATM security services for national security, aviation security, and law enforcement.

3.7 The DEN is an open forum type environment, and communication has to work both ways to be effective. All FAA ATC facilities and more than 60 other agencies and organizations participate on the DEN. While some facilities, agencies, and organizations may not participate 100 per cent of the time, they are required to be responsive to questions and provide information when called upon.

3.8 ATC personnel pass ATM security-related information via the DEN in accordance with FAA protocols. Information passed includes, but is not limited to:

a) aircraft in hijack status;

b) reports of unruly passengers or interference with crewmembers;

c) aircraft with inoperable transponder in the vicinity of the Washington, D.C., Special Flight Rules Area (SFRA);

d) aircraft communications lost or not established (NORDO);

e) aircraft transitions a Coastal Air Defense Identification Zone (ADIZ) and fails to land at the airport of entry;

f) inconsistent or abnormal aircraft activities;

g) aircraft deviates from route of flight and refuses to return to it when so requested;

h) any other situations that may indicate a suspicious aircraft activity or threat to aircraft or ATC facilities;

i) information concerning TOIs;

j) laser incidents and other surface-to-air incidents affecting aircraft;

k) reports of possible communicable diseases and other public health risks on-board aircraft; and

l) ATC facility status information.

3.9 Other agencies are required to report information on the DEN for:

a) unidentified Washington, D.C., SFRA and Coastal ADIZ penetrations;

b) unruly passenger/interference with crewmember reports;

c) “no-fly” passengers on aircraft approaching the United States;

d) unclassified intelligence that relates to NAS security;

e) aircraft incidents or accidents (aircraft not receiving ATC services);

f) bomb threats;

g) intercepts of suspect aircraft by DOD and DHS assets;

h) security incidents at airports (including laser incidents and surface to air incidents affecting aircraft);

i) reports of aircraft loitering in vicinity of sensitive facilities, i.e., nuclear power plants; and

j) reports of communicable disease or other public health risk on-board an aircraft.

3.10 In addition to the above items, agencies must report on the DEN when action is taken as a result of information received via the DEN.

3.11 FAA System Operations Security Air Traffic Security Coordinators (ATSCs)

3.11.1 *Headquarters FAA*

3.11.1.1 The ATSCs at FAA Headquarters have been delegated the authority to direct and coordinate with all Air Traffic facilities and regional offices to ensure system safety and security. To accomplish this, the ATSCs facilitate the interaction of Air Traffic facilities with the many governmental agencies that monitor the DEN.

3.11.1.2 The ATSCs have many years of aviation experience that encompasses both military and civilian ATC. All of the ATSCs have been air traffic controllers in FAA or military facilities. Many have experience as an FAA facility supervisor or facility manager or military commander.

3.11.2 *Continental US Region (CONR)*

FAA ATSCs are stationed at CONR to facilitate DEN operations and to coordinate directly with the Combat Command Officers.

3.11.3 *National Capital Region Coordination Centre (NCRCC)*

The primary mission of the NCRCC is to facilitate rapid coordination and information exchange among the participating agencies watching over the Washington DC National Capital Region (NCR). ATSCs perform ATM security functions that enable these agencies to fulfil their own air security or defence responsibilities in the prevention, deterrence and, where necessary, interdiction of air threats to the NCR.

3.11.4 *North American Aerospace Defence (NORAD) Command*

FAA ATSCs are stationed at NORAD to facilitate DEN operations and to coordinate directly with the Command Directors.

3.12 FAA ATC Facilities

3.12.1 The United States ATC system is a vast network of people and equipment that ensures the safe and secure operation of commercial, military and private aircraft. Air traffic controllers coordinate the movement of air traffic to make certain that planes stay a safe distance apart. Their primary responsibility is safety, but controllers also must direct planes efficiently to minimize delays and must report any ATM security related issues on the DEN.

3.12.2 Terminal controllers regulate airport traffic through designated airspaces; others regulate airport arrivals and departures. After each plane departs, airport tower controllers notify en route controllers who will next take charge.

3.12.3 There are 20 Air Route Traffic Control Centres (ARTCCs) located around the country, each employing 300 to 700 controllers, with more than 150 on duty during peak hours at the busiest facilities. Each ARTCC is assigned a certain airspace containing many different routes. En route controllers work in teams of up to three members, depending on how heavy traffic is; each team is responsible for a section of the ARTCC's airspace. A team, for example, might be responsible for all aircraft that are between 30 and 100 miles north of an airport and flying at an altitude between 6,000 and 18,000 feet.

3.12.4 The FAA's ATCSCC oversees all ATC. It also manages ATC within ARTCCs where there are problems (bad weather, traffic overloads, and inoperative runways).

3.12.5 FAA ATSCs interact with all these ATC facilities in real time via the DEN regarding all ATM security issues.

3.13 HQ FAA Washington Operations Center

3.13.1 The Washington Operation Center Complex (WOCC) is the cornerstone of the FAA Command, Control, and Communications System. The staff of the WOCC is trained to handle all of the agency's operational requirements. The staff is specifically structured to support all FAA Lines of Business (LOBs) which have operational responsibility to respond to events involving the following: natural disasters; facility security; hazardous materials; aircraft accidents and incidents; aircraft certification issues; air traffic operations; commercial space transportation; public affairs; congressional issues; National Transportation Safety Board (NTSB) interface; and international situations.

3.13.2 Of the operational responsibilities of the WOCC, the air traffic operation consistently takes the forefront in the day-to-day workload. The atmosphere following September 11 further highlighted the need to have a real time air traffic response to facilitate rapid, succinct crises management. Therefore, HQ FAA ATSCs are on duty at all times in the WOCC to manage the DEN, facilitate prompt responses to the Administrator and senior executives regarding ATM security issues, and support operational inquiries. The WOCC personnel assist the ATSCs in the exchange of critical information, verification of DEN participants, and connectivity to the DEN for all participants.

3.14 HQ FAA Air Traffic Organization (ATO) Incident Response Management Center (AIRMAC)

When activated by HQ FAA Air Traffic System Operations Security, the AIRMAC joins the DEN and serves as the ATO focal point for ATM security issues regarding national and international crisis management or disaster relief activities affecting the United States or its interests. If extensive airspace management for ATM security is required, the Airspace Access Response Cell (AARC) is activated and operates within the AIRMAC. The AARC manages airspace operations through direct communications with FAA air traffic security liaisons dispatched to the Federal Emergency Management Agency and to all Joint Operations Centres established for the crisis or disaster. In addition, the AIRMAC monitors response and recovery efforts. Based on input from DOD, DHS, and other partner agencies, the AIRMAC tailors airspace restrictions to insure safe, secure, and effective response and recovery operations.

— END —

ISBN 978-92-9249-289-2