Guide for Assessing Security of Handling and Issuance of Travel Documents

Version 3.4

January 2010

Executive Summary

The integrity of passports and other travel documents is a key component of national and international anti-crime and anti-terrorism strategies. Because travel documents can be powerful tools in the hands of criminals or terrorists, controlling the security of a country's travel document and its issuance processes directly impacts not only national and international security but also international respect for the integrity of the document.

In recent years, the rapid development of new technologies and new security techniques has led to a shift of travel document fraud. In the past, people who committed fraud concentrated on the end of the document production chain by falsifying or forging physical documents. Now, they concentrate their efforts at the beginning of the chain - document issuance systems as well as any kind of document register. Consequently, countries should be particularly concerned with the security of handling and issuance processes to help prevent the issuance of legitimate documents to terrorists or criminals under false identities.

At meeting No. 17 of the Technical Advisory Group on Machine Readable Travel Documents (TAG-MRTD 17), a project was approved to produce a common and practical guidance tool that would help ICAO Member States to either self-assess or assist in evaluating the security of another country's travel document handling and issuance system.

This guide is divided in two parts:

1) The first part recommends best practices to prevent and mitigate security threats at every step of the passport issuance process.
2) The second part provides a comprehensive evaluation tool checklist to assess the issuance process vulnerabilities.

The measures and practices presented in this document are recommended practices and as such no country is required to adopt them.

This guide was developed and will be maintained by the International Civil Aviation Organization Implementation and Capacity Building Working Group (ICBWG). Questions, comments and feedback on the guide should be addressed to the ICBWG at ICBWG@icao.int.

Document Change Control Table

Version Number	Date of Issue	Brief description of change(s)
1.1	Jan 07, 2008	1st draft
1.2	Jan 18, 2008	Structure modifications/editing—released to NTWG
1.3	April 10, 2008	Produced after NTWG Christchurch discussions, released to TAG
1.4	May 15, 2008	Update after TAG 18
2.0	Sept 30, 2008	Integration of comments and structure modification; released to ICBWG
3.0	March 10, 2009	Development of Part 2—Checklists Review and addition of text in all Chapters of Part 1 Harmonization of Part 1 and Part 2
3.1	June 29, 2009	Editorial changes
3.2	August 12, 2009	Comments Post Tavira and The Hague
3.3	October 2009	Final ICBWG comments from Cape Verde Meeting.
3.4	January 2010	TAG/MRTD comments from Australia

Table of Contents

Executive Summary 2

Introduction 6

A) THE ROLE OF TRAVEL DOCUMENTS IN NATIONAL AND INTERNATIONAL SECURITY 6
B) INTERNATIONAL CIVIL AVIATION ORGANIZATION (ICAO) 7
C) PURPOSE OF THE GUIDE 7

PART 1: Best Practices on Secure Issuance of TRAVEL DOCUMENTS 10

1 Travel Document Issuing Authority — Organizational Structure, Internal Security and General Security Practices 11

1.1 SUMMARY 11
1.2 ORGANIZATIONAL STRUCTURE 11
1.3 SECURITY FRAMEWORK 13
1.4 GENERAL SECURITY PRACTICES 16

2 Application Processes 19

2.1 SUMMARY 19
2.2 APPLICATION PROCESSES AND REQUIREMENTS 19
2.3 PHOTOGRAPHS 20
2.4 SECONDARY BIOMETRICS 21
2.5 TREATMENT AND PROTECTION OF PERSONAL INFORMATION 21

3 Entitlement Processes 23

3.1 SUMMARY 23
3.2 TREATMENT OF FIRST APPLICATIONS VERSUS RENEWALS 23
3.3 APPLICATIONS FOR CHILDREN 23
3.4 DOCUMENTARY EVIDENCE 24
3.5 OTHER MEANS OF IDENTIFYING APPLICANTS 26
3.6 TRAVEL RESTRICTIONS 28
3.7 ACTION WHEN ANOMALIES ARE DETECTED 28

4 Treatment of Materials and Blank Books 29

4.1 SUMMARY 29
4.2 BOOK PRODUCTION 29
4.3 NUMBERING 29
4.4 SHIPPING AND STORAGE 29
4.5 ACCOUNTING 30
4.6 DESTRUCTION 30

5 Personalization and Delivery 31

5.1 SUMMARY 31
5.2 PERSONALIZATION 31
5.3 DELIVERY 31

6 Document Security 33

6.1 SUMMARY 33
6.2 MACHINE READABLE TRAVEL DOCUMENTS (MRTD) 33
6.3 ELECTRONIC MACHINE READABLE TRAVEL DOCUMENTS (EMRTD) 33
6.4 ICAO STANDARDS, RECOMMENDED PRACTICES AND SPECIFICATIONS 35
6.5 TYPES OF TRAVEL DOCUMENTS 36

7 Facility Security 38

7.1 SUMMARY 38
7.2 PHYSICAL SECURITY POLICIES 38
7.3 SECURITY ZONES 38
7.4 ACCESS CONTROL AND MONITORING 40
7.5 OTHER PHYSICAL SECURITY PROTECTION AND PRACTICES 41

8 Information Technology Security 42

8.1 SUMMARY 42
8.2 IT SECURITY POLICIES AND PRACTICES 42
8.3 USER SECURITY 43
8.4 IT PERSONNEL 43

9 Protecting and Promoting Personnel and Agency Integrity 45

9.1 SUMMARY 45
9.2 SECURITY CLEARANCES AND SECURITY BRIEFINGS 45
9.3 WORK ORGANIZATION 46
9.4 STAFF MORALE [JOB SATISFACTION] 47
9.5 INTERNAL INVESTIGATIONS AND SANCTIONS 48

10 Lost and Stolen Travel Documents 50

10.1 SUMMARY 50
10.2 PREVENTIVE MEASURES 50
10.3 MITIGATION MEASURES 51

11 Overseas Issuance 55

11.1 SUMMARY 55
11.2 OVERSEEING OF WORK 55
11.3 ENTITLEMENT 55
11.4 PERSONALIZATION 55

12 National and International Stakeholders 57

12.1 SUMMARY 57
12.2 NATIONAL STAKEHOLDERS 57
12.3 INTERNATIONAL PARTNERS 58
12.4 PRIVATE PARTNERS 60

Reference Documentation 61

Abbreviations 62

Introduction

A) The Role of Travel Documents in National and International Security

Passports and other travel documents are internationally recognized official documents that show the identity and citizenship of a person for the purpose of facilitating travel abroad. They are used by border and immigration authorities to help determine admissibility and legitimacy of travellers who wish to cross international borders and enter another country's territory. They are also used by the issuing nation to grant re-entry into the country. The passport enables the holder to apply for a visa for those countries that require it upon entry, and allows the authority to annotate the passport, and record entry and exit dates.

In addition to travel purposes, passports are identity documents increasingly used for other types of transactions in the public and private sectors, such as opening bank accounts, supporting financial transactions, or accessing governmental services and benefits.

Travel documents, properly obtained or not, altered or counterfeited, are desirable tools for criminals and terrorist groups. In criminal hands, travel documents can be misused in an organized way to fund illicit activities, facilitate illegal migration, people smuggling and trafficking of humans, goods, or narcotics. A fraudulent passport can be used for espionage, financial crimes, flight to avoid prosecution or to facilitate other crimes. Such documents can also enable terrorists to travel—to recruit, network, mobilize, finance and organize internationally. Without the ability to travel freely that a travel document allows, terrorists can be impeded, localized, have their finances minimized and possibly even 'quarantined.' Consequently, their reach and impact is impaired. In effect, a passport, or other travel document, may be the security measure that prevents terrorists from reaching their target.

Criminals and their organizations are willing to pay large sums of money to obtain travel documents illegally, as well as to have access to the personal information that is collected, processed and stored as part of the document issuance process. This means that the integrity of the travel document and its issuance process can be extremely vulnerable to fraud, manipulation and malfeasance.

With recent, fast-paced technological developments, travel documents themselves have become more and more secure. More secure and difficult to forge documents lead to a shift of focus by fraudsters from counterfeiting and altering passports to seeking to obtain genuine documents by other illegal means. It is now recognized that travel document issuance systems will be targeted as will any kind of document or register that can be seen as breeder documents or authentic register (ie birth register.) Consequently, Travel Document Issuing Authorities (TDIA) as well as any organizations involved in the production of travel documents should be more concerned by the security of the handling and issuance process. A country may have a highly secure passport document, but if a person's identity cannot be established beyond a doubt or if a legitimate document is being issued to people who are not legitimately entitled to have it, the quality of the document matters very little.

Threats to the travel document issuance process can be broken down into several major types:

- Theft of blank documents and document materials to construct a fraudulent travel document (including unauthorized access to production and issuance facilities and/or unauthorized access to processing systems).
- Application for a travel document in a false identity using falsified, stolen or genuine breeder document.
- Application for a travel document in a false identity using manufactured false evidence of nationality and/or identity.
- Applications for multiple travel documents so that a traveller can hide previous suspicious travel evidenced by visas and entry and departure stamps from border officials.

- Use of falsely declared or undeclared lost or stolen travel documents.
- Staff malfeasance.
- Application for a travel document with the intention of giving or selling it to someone not entitled who resembles the true bearer.

Controlling the security of a country's passport issuance process has not only a direct impact on national and international security but also on the international respect accorded to the documents' integrity. The integrity of the document is paramount particularly when presented by citizens for visas and for border crossings. It may also impact the entry requirements of other nations. The level of security and the reputation of a passport can have serious repercussions on the convenience and expediency of international border crossing for citizens of that country. The integrity of the passport, and other travel documents, is a key component of national and international anti-crime and anti-terrorism strategies.

While passport integrity is necessary for national and international security, issuing authorities are also faced with the challenge of finding the correct balance between security, service, privacy and cost. However, fraud prevention is undeniably more efficient and much less costly than dealing with the consequences of successful fraud.

No country is immune from fraud yet, while it is impossible to eliminate 100 percent of threats and vulnerabilities, a combination of various features and methods can mitigate risk, keeping it an acceptable level and sufficiently deterring potential criminal interest.

This guide is an information tool for organizations involved in the travel document issuance process. It outlines security best practices and can also assist in assessing the security performance of the issuance process.

B) International Civil Aviation Organization (ICAO)

The *Convention on International Civil Aviation (Chicago Convention)* of 1944 established the International Civil Aviation Organization (ICAO). ICAO has long played a major role in establishing the standards, recommended practices and specifications for the issuance of travel documents. Section 3 of Annex 9 [Facilitation] of the Chicago Convention includes standards and recommended practices on passports and other travel documents.

In 1984, the Secretary General of ICAO established the Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD) made up of experts from several ICAO Member States. The TAG/MRTD develops and adopts specifications for MRTDs and eMRTDs, which are included in Document 9303. TAG/MRTD also publishes guidance material to assist States in implementing its specifications, as well as Technical Reports and Information Papers. Under the governance of the TAG/MRTD, two working groups were established: the New Technologies Working Group (NTWG) and the Implementation and Capacity Building Working Group (ICBWG).

At the seventeenth meeting of the TAG/MRTD in March 2007, a proposal for a Guide for Assessing Security Standards for Handling and Issuance of Travel Documents was presented and endorsed.

Web Resources:

⇒ ICAO MRTD Program: http://www2.icao.int/en/MRTD/Pages/default.aspx
⇒ Document 9303 (This document must be ordered from ICAO): http://icaodsu.openface.ca/mainpage.ch2

C) Purpose of the Guide

The importance of securing the travel document issuance process is well understood but guidelines on recommended prevention and mitigation measures are limited. "Is my issuance system

secure?"; "Which security measures are the most effective and efficient?"; "Where should I start?" are just some of the questions that countries and organizations involved in the travel document issuance process may ask themselves. In response, this guide provides a complete and simple security reference. It presents security best practices for preventing or mitigating threats and attacks to the issuance process. It also contains a self-assessment tool to help organizations identify their vulnerabilities.

This guide has been written from the perspective of passport issuance in countries without national identity cards or other universal national identity registration arrangements. In those countries where civil registration arrangements include a universal enrolment and/or identity card regime, passport issuance can be managed as a streamlined process that relies on the integrity of the prior enrolment for the national identity card. In these circumstances the checks and controls described in this guide for managing passport issuance remain essential, but are performed prior to an application for a passport, in a separate civil registration process. The content of this guide therefore remains relevant to all passport issuance systems, albeit the sections on enrolment and identity verification may need to be read as applying to civil registration as well as passport issuance.

Although the guide can be used by states to assess the security of the handling and issuance of their travel documents and make improvements where shortcomings are noted, the ICAO ICBWG strongly recommends the use of qualified assessors. The ICBWG can recommend assessors who are familiar with this guide and who have experience in all relevant aspects of the travel document continuum. Assessors conduct an objective and comprehensive in-country analysis of a state's travel document issuance process and prepare a confidential report for the requesting Government. The engagement of qualified assessors is essential where the state plans to use the report to seek capacity building assistance.

Several national and international organizations have been actively involved worldwide in outreach and capacity building activities to enhance the security of travel documents and their issuance processes. This guide recognizes the work of these organizations and is taking stock of their activities and realizations. In particular, under the auspices of the G8 Migration Expert Sub-Group (MESG) a paper called 'Minimum Security Standards for the handling of MRTDs and other passports' was produced and then adopted as Informative Annex III to Section III of Document 9303. This valuable document, which primarily addresses internal fraud, is the basis for the present guide.

Target Audience

This guide is meant to:

- guide policymakers of organizations issuing and/or involved in the production of travel documents in evaluating their own situation;
- support the ICAO ICBWG and other international organizations for outreach, capacity building assistance, or audit purposes;
- assist governments evaluate other States, i.e. States under consideration for visa-waiver eligibility.

Scope

This guide provides best practices and recommendations related to the issuance process for passports and other travel documents. Most of the practices and recommendations are equally applicable to other identity documents. The practices apply to both government and non-government organizations and facilities involved in all stages of the passport issuance process.

The measures and practices presented in this document are recommended practices, and as such, no country is required to adopt them. It is up to each country to determine, under its own legal, administrative, and policy framework, as well as cultural customs and traditions, the practices to adopt.

This guide addresses primarily the first step of the passport life cycle: the passport-issuance process. The issuance-process includes:

- intake;
- the decision-making and business processes to establish an individual's identity, citizenship and travel restrictions;
- production; and
- delivery of a document.

Note that the measures taken to enhance the security of the issuance process might also have a direct or indirect impact on other steps of the passport life-cycle such as the authentication, the validation and the repudiation.

Structure

Part 1 — Best Practices on Secure Issuance of Travel Documents recommends security best practices for every step of the passport issuance process. The first section is divided into twelve chapters.

Part 2 — Assessment Guide provides a comprehensive evaluation tool to assess issuance process vulnerabilities. It follows the recommendations and chapter organisation of Part 1.

Guide for Assessing Security of Handling and Issuance of Travel Documents

PART 1: BEST PRACTICES ON SECURE ISSUANCE OF TRAVEL DOCUMENTS

1. Travel Document Issuing Authority — Organizational Structure, Internal Security and General Security Practices
2. Application Processes
3. Entitlement Processes
4. Treatment of Materials and Blank Books
5. Personalization and Delivery
6. Document Security
7. Facility Security
8. Information Technology Security
9. Personnel and Internal Integrity
10. Lost and Stolen Travel Documents
11. Overseas Issuance
12. National and International Stakeholders

1 Travel Document Issuing Authority — Organizational Structure, Internal Security and General Security Practices

1.1 Summary

In general, the Travel Document Issuing Authority (TDIA) oversees the reception and processing of applications, determination of eligibility of applicants, production and issuance of travel documents.

While each chapter covers a specific aspect, step or phase of the travel document issuance continuum, this section focuses on the overall organizational structure and policy framework in which the issuance activities take place. These are the basics of an organizational environment supportive of security. Also discussed are security practices to be applied to all steps of the issuance process: regular threat and risk assessments and audits.

1.2 Organizational Structure

1.2.1 Mandate, Responsibilities and Legislations

The TDIA should be an independent governmental organization (or section) focussing only on the issuance of passports, travel documents and other government documents. There should be only one TDIA responsible for all the travel documents issued by the state. It should report to a senior executive level within the government which should be actively involved in ensuring that the mandate and responsibilities of the TDIA are carried out properly.

Laws or suitably enforced regulations are needed to establish the mandate, responsibilities, and the limits of authority of the TDIA, its senior officials and their staff. Many governments convert the general requirements of laws into specific regulations that have the force of law but also provide more detailed guidance to both the applicants and the issuing authority's staff as to what is allowable and where there is flexibility. Laws and regulations set boundaries for what the applicant can expect to receive and what staff members can legitimately provide under their own authority. Authorities at the national, regional and local levels should all be clear. Areas to be regulated should be:

- basic authority to issue, revoke, withhold, recover, cancel and refuse travel documents;
- who may apply for a travel document
- the requirements that must be met by applicants who wish to obtain the document;
- fees for the services provided by the issuing authority;
- record keeping requirements;
- privacy protection;
- the validity period of the travel document
- information to be provided in the travel document
- instructions on the use of travel documents; and
- mechanisms to prosecute forgery, improper use of travel documents, false representation – use of someone else's travel document, and mutilation of the travel document.

Because of its security implications and interrelations with border control and immigration functions, the travel document issuance function should be included in the national security framework of any country and be recognized as having a significant impact on national and international security. A desirable result of this recognition is that the security responsibilities of the issuing authority be adequately supported and resourced by the government. The TDIA and its staff should be involved

in the governmental security planning at large and be aware of the global impact of their security responsibilities.

1.2.2 Structure of the Issuing Process [centralized or decentralized]

Each government needs to come to its own conclusion as to the most appropriate structure to use for its issuing process, whether it be centralised or decentralised, based upon considerations of workload, geography, social situation, security, required level of customer service, etc.

A uniform application and issuing process at all travel document personalization and issuing locations is highly recommended to make the process standardized and transparent. By using standardized forms, software and hardware configurations and procedures it is easier to guarantee a minimum level of quality, compliance, security and control. No matter the structure chosen, there should be centralized supervision and control of all aspects of the issuance process. Routine reviews and audits in all organizations and facilities involved in the passport issuance process are critical.

1.2.3 Use of Partners [public or private]

Many countries are using partners (government partners or reputable outside vendors) to perform some of the travel document issuing functions. These can include:

- book production (or material used in book production);
- reception of travel document applications;
- printing; and/or
- delivery.

Entitlement decisions should NEVER be outsourced.

In deciding whether to use public or private partners, several factors must be taken into account. The following table presents some key considerations. Each issuing authority should come to their own conclusion based on their particular situation.

Factors	Comments
Costs	The costs of the functions may vary if performed in-house or outsourced.
Availability of resources	The issuing authority may not have the internal resources, e.g. human, facilities, equipment, to carry out some of the functions.
Accessibility of service	Depending on the territory covered by the issuing authority, services may be more accessible to the population if performed by partners.
Control of data, material and processes	Outsourcing can prove less desirable from a control perspective unless this control is specifically retained/regulated within a contractual agreement.
Location, nationality of outsourced companies	Legitimate political, economic and security context should be taken into consideration.
Transportation concerns	The security of travel documents/materials while in transit is critical.
Security measures implemented in facilities	All facilities involved in the issuing process should have adequate on-site security and safeguards.

Before the country begins to tender for a new travel document, production and issuing systems or other services, it should carefully plan all the aspects of the project. In many instances, the success of the overall project depends on the preliminary work done in the planning phase of the project. Extensive benefit can be gained from pre-project research. Countries should contact other

countries who have implemented the system or service being considered in order to learn from their experiences. Another good practice is to proceed with a Request for Information (RFI) to establish what types of systems and technologies are currently available to better determine the needs of the issuing authority. Before entering into an agreement with a potential partner, a Threat and Risk Assessment (TRA) of the partner should be done in order to ensure the reliability and security of that partner. Once a partner has been selected routine audits must be done throughout the duration of the working relationship.

Contracts or memoranda of understanding should be in place describing the rights and responsibilities of all the parties involved, and the penalties if these are not respected. The TDIA should conduct regular reviews and audits of partners to ensure that they have adequate on-site security and safeguards. Regular risk assessments on all facilities are recommended.

1.3 Security Framework

A security framework includes the security strategies, policies, practices and controls contributing to a more secure travel document issuance process. As an example, the aim of the present guide is actually to assess the security framework of a TDIA. The security framework promotes a better coordination, standardization and coherence of security concepts and practices within the organization and the document chain. Some basics must be in place to ensure that a security framework is in place, effective, known and followed by staff and management. This section presents these basics, which include a dedicated security team, documented policies and guidelines, management and financial support and training and awareness tools and activities.

1.3.1 Security Team (or Section Dedicated to Security)

The TDIA should have a team or a section responsible for and dedicated to developing, overseeing and ensuring the compliance of the security framework. This security group should be independent of the operations. The staff of this section should receive appropriate resources and up-to-date security training. The responsibilities and activities of the security team should be well planned and reported to senior management. They should include (but not be limited to):

- defining the security framework—strategies, policies, practices and controls;
- performing documented security reviews, risk assessments and audits of all facilities and processes, as well as of partner organizations;
- ensuring the integrity of the travel document issuance process;
- ensuring the security and quality of the travel document;
- providing expertise in fraud;
- developing security training and awareness programs;
- performing internal investigations in the case of security incidents; and
- consulting with governmental stakeholders, e.g. border control, immigration, law enforcement, on security issues.

1.3.1..1Internal Controls Manager

Every organizational change, technology upgrade, modification to the application process, and operational method may have consequences for the security of the issuance process. Therefore, it is important to have senior managers designated at the national (headquarters) level, and at each production site (field office), to make certain that security and internal control considerations are factored into management decisions.

These managers should be independent of the operational chain of command and ultimately report to the head of the issuing authority. The reason for independence from operations is that the

primary responsibility of the operations office is to issue travel documents, prevent backlogs, and get the workload completed. While that does not preclude concern for internal controls, it will not be the first concern of operations.

- At the national level, the designated internal controls manager should be a senior manager who is a participant in the planning and decision-making levels of the organization.
- At the field office level, a senior officer should be designated as responsible for internal controls, preferably someone who knows the work in detail but who has no authorization in application or document processing. Successful administration of the site's internal controls program should be a critical element in that officer's performance evaluation.

1.3.1..2 Anti-Fraud Team

It is recommended that the TDIA create a team with a primary focus on fraud prevention. There should be at least one representative of this team in every passport issuing office.
The tasks of the anti-fraud team would include:

- coordinating anti-fraud operations;
- providing training resources;
- providing advice on difficult casework;
- liaising with other government entities that produce breeder/primary and supporting documents; and
- liaising with other governmental agencies that prosecute fraud when it is found.

1.3.2 Documented Security Policies

The security policies, practices, guidelines and strategies developed by the security section and which form the organizational security framework, should be written and documented. They should include the procedures and internal controls that have been developed to minimize vulnerabilities in all aspects of TDIA operations. They should be fully and consistently implemented in all facilities and partner organization involved with travel document issuance.

The policies practices and guidelines should outline the responsibilities of all individuals with regard to the security of assets and emphasize management's support of the security program. They should be communicated to all employees so that they are well known. They should be easy to refer to and easy to understand. Compliance with policies should be closely monitored and the policies should be strictly enforced.

The information in each of the subsequent chapters can form the basis of security policies and procedures.

1.3.3 Management and Financial Support

1.3.3..1 Management Support

No security program can work properly without support from senior management. Decision makers must be willing to commit time and resources to the development, implementation and maintenance of an effective internal controls system. Implementing such a system may require reorganizing workflow, changes in personnel administration, revisiting other aspects of operations, organization of training and awareness sessions, etc. It is also vital that senior management set the example by following the security policies and other measures set by the security team, by not breaking the rules, and by not asking for special favours.

1.3.3..2 Financial Support

Dedicated resources, e.g. money and staff, are also required to protect the integrity of the issuance process. This can pose difficulties to an issuing authority that operates on a small budget. However it is important to realize that the failure to provide adequate resources to sustain an effective internal controls program can ultimately lead to major costs. They may include:

- the potential for national embarrassment should a country's travel document be used in committing terrorist acts:
- the difficulties that a country's citizens will have in international travel if their travel documents are more closely scrutinized by foreign border and visa authorities; and
- the substantial costs that are incurred in investigations, prosecutions and incarcerations stemming from criminal activity facilitated by travel document fraud.

A high-quality document issued with a high level of integrity will go a long way to preventing these types of abuse. The cost of prevention through a highly secure and controlled issuance process is generally much less than the cost of dealing with the results of an insecure issuance process.

It is recommended that the process for setting fees for travel document services take into account the actual cost of providing travel document services, including the necessary cost of security in all its forms, e.g. personnel, training, software, hardware, materials, physical security, stationary, brochures, communication materials and maintenance equipment.

1.3.4 Establishing a Culture of Security [Training and Awareness]

The organization needs to promote security of its staff in order to develop an organizational culture conducive to the implementation and respect of security policies and practices. The following are some examples of techniques that could be used by senior management to develop a culture of security and to enhance the security awareness of its staff:

- regular security training, information sessions and refreshers;
- regularly remind individuals of their security responsibilities;
- development of a code of conduct/values and ethics guidelines (Chapter 9);
- communication and advertising campaign on security policies;
- publication of results of security assessments and audits;
- organization of monthly meetings on security;
- production and distribution of intelligence bulletins;
- use of the intranet;
- use of positive reinforcement and rewarding of good security practices; and
- imposition of sanctions and disciplinary actions for non-compliant or negligent behaviour.

It is important to provide regular security training to maintain employee security awareness. Depending on their position, staff should also be trained on specific security measures that apply to their functions such as document abuse, counterfeiting and other aspects of fraud. They should also be trained in handling personal information and privacy, as well as IT security. Staff understanding of the security concepts and practices and of the reasons behind them should be verified. If personnel lack information or do not understand the necessity of all the security steps to be carried out, they may try to find ways to make their job easier by finding shortcuts in procedures. Staff should also be encouraged to make suggestions on possible improvements to security practices.

1.3.5 Performance Standards

The position descriptions of all staff should include a standard of performance that imposes a requirement to be aware of and adhere to internal controls. Assessment of all staff should include

an evaluation of internal controls performance and disciplinary measures in the case security duties or responsibilities are neglected.

1.3.6 Workload Anticipation and Planning

The TDIA should forecast surges in travel document applications and plan financial and human resources accordingly. Projection of future workloads can be achieved by using historical data and factoring in known elements that may impact on document production demands, e.g. traditional travel periods such as school holidays, major events, the economy, and the requirements of other countries for entry, etc.

Every effort should be made by the issuing authority to establish an adequate staffing level to meet projected workload demands. Contingency plans to deal with excess sickness, e.g. pandemic, should also be prepared. The capacity should not be increased too quickly to avoid having an important number of new and freshly-trained employees. The TDIA should maintain a group of pre-cleared /background checked call-up resources to use in case of overload or understaffed situations.

Internal controls are more important than ever when there is an increased workload because staff concerned with customer service and backlogs of applications may be tempted to cut corners or ignore internal controls procedures that may be seen as slowing the movement of the work. When under pressure of demanding workloads, managers must resist the impulse to ignore internal controls.

1.4 General Security Practices

Some security practices apply to the whole travel document issuance process: Threat and risk assessments and audits should be performed regularly on all steps, functions, assets and facilities involved in the issuance process. These practices are explained in the present section ‘General Security Practices’ instead of repeating their importance in each of the subsequent Chapters.

1.4.1 Threat and Risk Assessments

It is recommended that the TDIA take appropriate action to risk manage the security threats and vulnerabilities to its issuance system. Risk management is the process by which resources are planned, organized, directed, and controlled to ensure the risk of operating a system remains within acceptable bounds at optimal cost. Because it is prohibitively expensive, and probably impossible, to safeguard information and assets against all threats 100 percent of the time, modern security practice is based on assessing threats and vulnerabilities with regard to the degree of risk each presents, and then selecting appropriate, cost-effective safeguards.

Regular threat and risk assessments are important as they help determine current threats to the issuance system and which assets and areas are most at risk within a process. Assessments lead to recommendations for prevention and mitigation measures that will reduce risks to acceptable levels. Threat and risk assessments involve:

- Establishing the scope of the assessment;
- Determining the threats, and assessing the likelihood and impact of threat occurrence;
- Assessing the risk based on the adequacy of existing safeguards and vulnerabilities; and
- Implementing any supplementary safeguards to reduce the risk to an acceptable level.

Threats and the underlying reasons for attempts at fraud may differ significantly from country to country, and even region to region. This is why threat and risk assessments should be performed on all issuance facilities and on all stages of the issuance process in collaboration with law

enforcement authorities. It is important to note that threats also come from internal sources and the TDIA needs to ensure that processes and systems for supporting staff and managing risks for misconduct and corruption are covered.

The people who know best what the vulnerabilities are, are the people who work with the systems and procedures. It is wise to ask the staff periodically what they think the vulnerabilities are, and what should be done to minimize them. Reporting of concerns should be encouraged and there should be appropriate recognition for those who identify problems. It is good practice to maintain statistics on threats or risks that materialize in order to focus resources on making changes in the process to prevent future incidents or attacks of a particular type.

The organization must continuously monitor for any change in the threat environment and make any adjustment necessary to maintain an acceptable level of risk and a balance between operational needs and security. For more information refer to the Australian and New Zealand Risk Management Standard ASNZS 4360/2004, which is currently evolving into ISO 31000 (http://www.iso.org/iso/catalogue_detail.htm?scnumber=43170).

When considering risks and vulnerabilities the TDIA should also develop a Business Continuity Plan to ensure that, if a major threat or attack materialises, passport operations can continue. This is particularly important for States with one primary issuance site. For more information on Business Continuity Planning, refer to good practice guidance material and standards at the Business Continuity Institute (http://www.thebci.org/).

1.4.2 Audits

One of the most effective means of ensuring employee compliance and understanding of the rules established to prevent fraud is to have a system of formally required audits. There should be periodic and ad hoc internal audits as well as audits performed by external independent organizations.

1.4.2..1Internal audits

Formal and ad hoc audits should be performed regularly in all facilities and for all steps of the issuance process to ensure policies and rules are being followed.

Formal internal audits and compliance reviews should be done by senior officers to review operation management and the adequacy of the internal controls program. A formal report of findings should be produced by the inspection team and their recommendations for improvements should be sent to the senior executive to whom the TDIA reports. There should be a compliance process in place to ensure that needed changes are implemented.

These formal audits should be supplemented with active review of work in progress by managers. Work in progress should be randomly checked to ensure that established rules are complied with. This is true at all times but especially in periods of high workload when staff and management may be tempted to cut corners and ignore some internal controls. Internal reviews should require senior officers in all facilities to look at a percentage of the most urgent applications, other applications in process, and applications for travel documents already issued to verify that proper procedures have been followed; that evidence attached or recorded is adequate; that notations are complete; that actions directed can by justified; and, that proper fees have been paid.

1.4.2..2External audits

An external and independent organization such as the governmental audit office should also carry out regular performance audits to evaluate the security practices of the TDIA. These independent organizations will usually produce recommendations and are responsible for monitoring their implementation. External audits prove to be very effective as they are not blind to Usual Practices

within the organization, are not influenced by operation requirements, and are aware of security threats and other effective security measures in place in other organizations.

2 Application Processes

2.1 Summary

To obtain a travel document, applicants must follow a specified application process, including the completion of forms, documentary evidence, submission of photographs, and in some cases secondary biometrics. The information and documentation they provide will enable TDIA employees to establish the entitlement of the applicant to a travel document.

The information the applicant submits must be protected during the whole issuance process and also after the travel document is issued. Privacy and protection of data are essential elements to ensure the security of the travel document issuance process.

2.2 Application Processes and Requirements

2.2.1 Uniformity of the Processes

No matter what the organizational structure of the TDIA, i.e. centralized/decentralized, and no matter what the information and documentation to be submitted by the applicant, all applications should be processed in a uniform manner throughout the TDIA. All application forms should be standardized and the requirements the applicant must comply with should be consistent across the country. Policies and procedures covering how and where to apply should be easily accessible by the public. The whole application process must be transparent. Policies and procedures on how applications should be processed should be documented and readily available to TDIA staff.

2.2.2 Factors Affecting the Process

The application processes and application requirements do vary from country to country, and will be a matter for each state to decide, e.g. applications in person, by mail, online, etc. Several factors, in addition to security, are to be taken into consideration when establishing the application processes, including:

Factors	Comments
First application or renewal	A first-time application should be scrutinized more carefully. Applicants who have had a previous passport may not be required to appear in person or to submit the same documents, i.e. breeder documents, as a first time applicant, but usually they must include their previous passport (or travel document) in their application. However, if this previous passport is in a false identity, automatic renewal without additional verification perpetuates the problem.
Accessibility of service	Depending on the territory covered by the issuing authority and the network of TDIA offices, the option of mailing the application or applying at partner's offices may provide a more accessible service for the population.
Identity confirmation	A required appearance before some sort of governmental official offers a better chance of identity confirmation for the wide range of applicants. First it can be confirmed that the person is still alive, photographs can be compared to the live person, questions can be directly answered by the applicant, and the personal comportment of the applicant can be observed and judged.
History of lost or stolen travel documents	If the applicant has a history of lost or stolen travel documents, he may be required to apply in person (Chapter 10).
Collection of secondary biometrics	Biometric capture necessitates the presentation of the applicant in person on at least one occasion.
Security of the mail system	If public or private mail delivery services cannot be trusted, the application process should require applicants to apply in person.
Technology	Development of new technologies can enable some parts of the application process to be done online or remotely, e.g. printing or forms, transmission of data, transmission of digital photographs, interviews by telephone or teleconference.

Urgent or express service	Applications that must be processed urgently may require the applicant to apply in person at a TDIA office.

Many countries require personal appearance for every travel document application, including renewals, but whether that is necessary depends on the safeguards in the whole application and issuance process. Some countries require only those applying for the first time, children under the age of majority, and persons who cannot present their most recent prior travel document to appear in person to apply for a new travel document. Adults who have already had their identity authenticated can be properly identified by matching their old passport with new photographs (and biometrics) and may not necessarily need to appear in person. From a security perspective, requiring appearance in person helps increase the security of the process. However, other means to verify identity can effectively mitigate the security risks to an acceptable level.

Travel document application acceptance agents, if they are used at all, must be trained and should have detailed written guidance on how to identify passport applicants, how to note the identifying documents on the passport application, and what to do in the event that they are not satisfied with the identity documents presented. Staff should be trained in other skills that will help to highlight other signs or indicators of a fraudulent application, for instance: interviewing skills, body language recognition skills, verification of breeder documents, and the ability to see inconsistencies in the totality of the applicant's presentation and documents.

In many countries, travel document applications are accepted by partners outside the issuing authority. The partner may simply act as a post box carrying out very basic checks to ensure that the application has been completed fully, that a fee has been paid and that documentary evidence where required is included. If not carried out by the issuing authority, it is recommended that this function be assigned to governmental institutions that are familiar with legal processes and paperwork, such as courts, police, post offices or other government offices that are used to dealing with the public such as tax offices or government operated libraries. Partners of the passport authority should be trained to perform verification of breeder documents and provided with elementary training in fraud characteristics and detection. In case of doubt, cases should be referred to the TDIA.

2.3 Photographs

The issuance of travel documents requires the applicant to submit photographs. These photographs could be taken by a commercial photographer, trusted partner or country official. Only photographs which meet the ICAO specifications included in Document 9303 should be accepted by the issuance authority. Respect of these specifications facilitates the identity verification of the holder by the TDIA and at the border and also permits the use of facial recognition technology. To help ensure compliance with the ICAO photo specifications they should be made available to commercial photographers as well as the public.

The following are examples of published photo specifications:

US: http://travel.state.gov/passport/guide/guide_2081.html
New Zealand: http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Passports-Photographic-Requirements
Canada: http://www.pptc.gc.ca/cdn/photos.aspx?lang=eng

With the development of new technologies, some countries may start accepting online applications and digitized or electronic photographs. These photographs should be taken by a trusted partner or country official and transmitted securely from the point of capture to the issuing authority without an opportunity for alteration. To minimize the risk of the photograph being altered at various steps of the application process, a hard-copy photograph should be required in addition to the digitized photograph.

2.4 Secondary Biometrics

Many countries require, or will require collection of fingerprints as part of the travel document issuing process. Biometric collection, including fingerprints or iris, if carried out by a country, may be done in a number of ways: by issuing authorities, by other government officials, by third party trusted agents appointed by government or some other secure and trusted means. The handling of biometric collection or enrolment will be a matter for each country to decide. Whichever method is selected, the imperative must always be that the method shows respect for privacy and is demonstrably secure and trustworthy. The country must decide if the collection of biometrics is required only for a first application or for every travel document application including renewals.

2.5 Treatment and Protection of Personal Information

To effectively perform its mandate, the TDIA is processing and storing vast quantities of an applicant's personal information. This information needs to be rigorously safeguarded as criminals will seek to access and use it for illegal purposes such as identity theft, financial gain or other types of identity fraud. These types of fraud are more and more prevalent, and are now a great concern within society.

The travel document application form, when completed, contains some personal information. This information is usually protected by privacy laws and should not in any case be disclosed to third parties without appropriate authority. TDIA staff should be given training and documentation on the various information and privacy laws effective in their country and management must enforce these laws. In addition to privacy concerns, unauthorized communication of this information to outside parties can lead to identity fraud.

Every application should be logged at first receipt and its status updated throughout the processing chain. All individuals involved at different stages in the application handling process should be identified on the status log record and appropriately Signed Off when the application passes to the next step. This permits high-level overview of who has accessed the file and control of the status of the application at all times. This is particularly important for "Very Important Persons" (VIP) files. All forms and documentation submitted should be stored in appropriate, locked filing cabinets or, at least, kept in a secure location at all times including when being processed. It is essential that, outside of normal working hours, pending work be locked up so that building guards, other employees, or cleaning staff will not have access to the private information of applicants. Staff should always be able to account for every application document and copies. Such documentation should never be removed from the TDIA facilities.

Personal application details that are kept on computerized records must be protected by appropriate IT security standards (Chapter 8) and should never be safeguarded or shared through an unprotected network, internet connections or portable devices that could be removed from the TDIA facilities. Electronic log records are to be used to control and track access to the file. For additional security, features such as biometric controls or personalized identity cards may be used to access a system or database.

After application processing is complete, all application materials containing personal details of the applicant (including application documents, computer records, breeder document images and data, images of the data page, as well as the chip contents of ePassports) should be carefully and securely stored for ease of future reference in appropriately locked cabinets or protected rooms and in appropriate security-protected databases. Access to the archived records should be subject to strict permission control and access logging and tracking. When information is no longer required, it should be destroyed using appropriate shredding or document destruction devices in compliance with all TDIA and governmental laws and policies on record keeping.

2.5.1 Automated Systems

Using technology to automate passport issuance processes can increase the security of the passport issuance process and enhance accuracy. Data entry, scanning, printing, archiving, mailing and management reporting processes can all be automated to a certain degree. This limits the involvement of manual manipulation of data, and may improve the rapidity of detection of fraudulent or questionable information. Automated systems can include a random-security checking function that requires the application to be seen by a supervisor before the application is authorised for issue.

3 Entitlement Processes

3.1 Summary

In most countries there are three necessary elements that a government needs to establish before issuing a travel document: evidence of the applicant's identity, i.e. this is a real identity and the applicant is in fact the claimed individual; proof of citizenship; and, verifying if the applicant is subject to any travel restrictions, e.g. criminal record, history of lost and stolen travel documents, failure to pay child support, etc. Several tools and techniques are used to help determine entitlement to travel documents. The uses of such tools and techniques vary from country to country. There is no single method of firmly establishing identity but there are various ways by which a reasonable certainty of authentic identity can be established. To verify identity and citizenship, documentary evidence is usually required by the TDIA. Additional strategies include the collection of biometrics, verification of social footprint, use of a guarantor and references, interviews, etc.

Applicable travel restrictions that do not permit or restrict travel for certain individuals are usually verified by screening applications against watch list databases containing information collected from the TDIA and various partner organizations.

The TDIA should have documented policies and procedures related to verifying identity and determining entitlement to a passport. These policies and procedures should be readily available to TDIA staff and compliance with the policy and procedures should be monitored.

All entitlement decisions should be made by appropriately trained TDIA staff.

3.2 Treatment of First Applications versus Renewals

In some countries the application and entitlement process is different for first time applicants and renewals. The information and documentation required may differ as well as the verifications undertaken. Countries that use a different process for applications for renewals should have a policy which clearly defines under what conditions an application for renewal can be submitted i.e. previous passport expired less than one year before the application for renewal.

(Example: Simplified Renewal Process at www.passportcanada.gc.ca/cdn/ren.aspx?lang=eng)

First applications should be scrutinized more carefully. Countries that allow renewal applications to be submitted a long time (i.e. over 2 years) after expiry of the previous travel document should scrutinize these applications more closely as well. In the case of all renewals, application data submitted should be compared to details of the travel documents previously issued to that individual. Also, for renewals, if the previous travel document was issued under a false identity, automatic renewal perpetuates the problem. Additional verifications such as database checks and reference checks should be performed to ensure this would not happen.

3.3 Applications for Children

A travel document application for a child should be lodged by at least one parent or other person with a parental responsibility for the child. Evidence of birth and of a social footprint should be provided, along with potential comparison to other supporting documents if the child is old enough to qualify for them. The parent(s) or other person with parental responsibility lodging the application must establish their identity. Children shall not be

included in an adult's passport; rather, each child, including a newborn infant, must be issued with his or her own passport.

3.4 Documentary Evidence

Confirmation of the identity of travel document applicants is key to document integrity. The applicant, to identify himself or herself, uses a document or a combination of documents. In addition to the identity, the documentary evidence should also demonstrate the citizenship of the applicant.

It is crucial to establish that the identity claimed is a real identity that belongs to a living person and does not in fact belong to a deceased or entirely fictitious person. The identity of a deceased person can be misused by impostors to enable a fraudulent document application. Steps should be taken to ensure that claimed identities belong to the living individuals who claim them.

Documentary evidence to establish entitlement under identity and citizenship requirements can be combined in a single card or document:

- Birth certificate
- Marriage certificate
- Certificate of citizenship
- Certificate of naturalization
- Existing passport or other travel document
- National ID card

These documents are called breeder or primary documents. Breeder documents are those that bear identifying details and nationality and are issued by a trusted government or other official source. They have already been subject to a sufficiently high level of verification by trusted personnel before being issued. The breeder document should contain basic security features including a unique number and potentially a biometric or clear photograph. Without those features, the TDIA is vulnerable to the theft of the card or identity of a living or dead person. A document that does not contain a photograph or biometric is generally not acceptable as evidence of identity when presented in isolation. This type of documentation can however contribute to the overall evidence of identity when presented along with other forms of documentation. In such cases, the applicant will be asked to provide supporting documents to confirm, for example, that the applicant is a living person who lives at a specific address. Examples of supporting documents include:

- Identity card
- Register of electors
- Census record
- Medical record
- Social security and tax record
- Employment record
- Drivers' licence
- Motor vehicle ownership record
- Financial record

There should be special procedures defined for dealing with applicants having only limited breeder and supporting documents, e.g. older birth certificate, no driver's licence, etc. Other means and techniques to validate identity are particularly important in these cases.

Applicants must submit their documentary evidence with their application. Original documents should be handed over, scanned by the TDIA and kept in the central database so that it can be verified by unannounced audit at any time during the entitlement and issuance process or at the time of a renewal. It is then returned to the applicant with the issued travel document. For renewals, some countries are not asking applicants to resubmit their documentation, except the previous

passport (or other travel document) and verification is done using the information and scanned documents already included in the TDIA database.

In many countries, the documentary evidence used (breeder and supporting documents) is issued, stored and retrieved separately. It is often issued by local or regional authorities with little or no national standardization or control. Such documentation often contains few security features. Persons who would obtain travel documents in false identities can use many methods to obtain breeder documents—they can engage in identity theft, taking advantage of loose application procedures; create false identities based on deceased individuals; or counterfeit reasonable facsimiles and fill them in and present them as genuine. Special care should be given to the verification of the authenticity of the documents presented by the travel document applicant.

It is recommended that the identity of the claimers be verified against paper or electronic death records.

The New Zealand Government's Authentication of Identity Standard is a useful reference: http://www.e.govt.nz/services/authentication/standards/index.html

3.4.1 Verification of Document Authenticity

3.4.1..1 Verification of security features

Staff accepting applications and adjudicating entitlement to travel documents should be trained in both the characteristics/security features of genuine documents and the identification of false documents. Breeder documents, often birth certificates, probably exist in many different forms within a country. This complicates the identification process related to the issuance of travel documents.

Ideally, the issuing authority's own trained and appropriately security cleared staff will perform verification, but the larger the country is and the more application locations there are, the more likely it will be that the issuing authority may partner with other organizations that are well represented locally. Partners of the TDIA should also be trained to perform verification of breeder documents. In case of doubt, cases should be referred to TDIA personnel for appropriate advice and guidance. It may be necessary for applications accompanied by specific types of less reliable citizenship/identity evidence to be routinely referred to supervisors and to the fraud unit for review and document checks. Prescribed security minimums should be given to all examiners.

3.4.1..2 Document databases

There are government owned and commercial databases available that contain examples of a variety of genuine breeder documents or travel documents. These databases can be used to verify the authenticity of the documents submitted by the applicant. DISCS for breeder documents and EDISON for passports are examples of government-owned databases available, for a fee, to all issuing authorities worldwide.

3.4.1..3 Reference to official records

Wherever possible, direct electronic access to appropriate and secure government records or registers should be sought rather than viewing hard copy documents.

An automated check on each application can significantly help detect and prevent fraud. Examples of automated tools are online verification with primary source document agencies, e.g. birth or citizenship records, birth and death record databases, commercial license registries, voting rolls,

property ownership records, and/or motor vehicles records. This will help confirm legitimate documents and rapidly identify fraudulent ones.

When electronic links do not exist, it is recommended that the TDIA contact the breeder/primary document issuers on a regular basis, randomly or in cases of doubt, to verify the integrity of documents submitted by the applicant.

3.5 Other Means of Identifying Applicants

It is also recommended that the use of other means of identifying individuals be used as this improves confidence in the confirmation of identity.

3.5.1 Interview

If the TDIA requires an appearance in person of the applicant or if there are any doubts regarding the integrity of the information and documentation provided, interviewing the applicant can be useful. TDIA officers should be trained to determine prima-facie identity, judgment of personal mannerisms and confidence of applicant. Similarity of the applicant with the photos submitted with the application can be verified. Personal questions can also be asked to verify if there are any inconsistencies between the application and the answers provided at the interview.

3.5.2 Guarantor

Where interviews are either not carried out or are not possible a helpful method that has been successfully used in some countries to support a claimed identity is a process of designating professionals such as doctors, lawyers, clergy, etc. to countersign applications attesting to the identity of the applicant. If the professional has known the applicant personally over many years, this can be an effective means of identification. Professions selected to act as counter-signatories should be those that maintain records of membership through a recognized association and that can be verified by the TDIA. There is a drawback, however, in that it is difficult for the issuing authority to keep track of all the people authorized to countersign.

Some countries use guarantors that are not members of recognized associations but are travel document holders. With this method it is easy to verify the personal information of the guarantor—information that should be included in the TDIA database. Document-holding guarantors must have known the applicant personally for a long period of time and agree to witness the applicant's identity in written form, under oath or penalty of perjury.

Guarantors must not be paid by the applicant for acting as guarantor. This policy should be indicated on the application form and should require the guarantor's acknowledgement with his or her signature. One of the applicant's photographs should also be signed and dated by the guarantor as being a true likeness of the applicant.

To verify their statements, guarantors should be contacted on a regular basis by the TDIA, or, in case of doubt, concerning the identity of the applicant. For security reasons, it is not recommended that guarantors be closely related to the applicant, e.g. siblings, parents, children.

3.5.3 References

In addition, or in the absence of the use of a guarantor, personal references (independent and unrelated to the applicant) having known the applicant for a long period of time, may be used. At least two references are recommended. These references may be contacted by the TDIA to verify the identity claimed by the applicant.

3.5.4 Social Footprint

A Social Footprint is the impression each individual leaves within the community by their personal involvement in the events or interactions within society. Even those who lead extremely low-profile lives will have left some form of impression within present day society. Such information, usually built over a long period of time and through a combination of varied sources, is difficult to falsify successfully. As far as possible or practical, the TDIA should seek to establish the mark left in society by any individual applicant. Technology increasingly facilitates the use of whatever reliable information is available to cross-reference data to substantiate the background of any claimed identity. Useful areas of enquiry to support the ownership of a claimed identity are the use of credit reference agencies, other financial records/information, parental details, health or educational (school/college) records, details of previous or current employment, tax records or current/previous residence details among others.

3.5.5 Use of biometrics

Biometric technologies confirm the physical features of an identity claimed by the person whose biometrics are used whether the identity claimed is genuine or not. Once assigned, biometrics limit the individual to one specific identity and curtail ability to travel or to obtain other travel documents of the issuing state using multiple identities. Authentication of identity is therefore particularly important before any biometric information is attached to that identity. In developing a biometric enrolment process, it is important to keep in mind that there should be adequate safeguards to ensure that the identity of the enrolee is properly established and thoroughly documented before permanently fixing the identity to the recorded biometrics.

3.5.5..1Facial Recognition

Facial Recognition (FR) technology can be used by the issuing authority as a tool to eliminate the possibility of applications being made by the same person in differing names. This technology can also prove very effective when it is used before issuance of a document against a Watch List or gallery of “undesirables” or known document abusers. Comparison with the existing gallery of images can therefore deny the would-be impostor successful ownership of more than one document. As stated in Chapter 2, to enable this technology to perform at optimum level, it is important that images used at the time of application for the document meet the international interoperable specifications laid down by ICAO.

3.5.5..2Other Biometrics

Collection of other biometrics (fingerprints or iris) can also be done as part of the issuing process. For applications for travel document renewals, biometrics from the applicant can be compared with those collected previously to verify that the identity used is the same.

3.5.6 Database Checks

Applicants should be checked against the TDIA database (or archive where no electronic database exists) to ensure that the individual does not hold other travel documents under a different identity. The database should be checked for similar names, spelling and biographical data.

The system should be designed so that two types of searches are performed on applicant data: matches, and potential matches. The latter occur because something in the database (common names, for instance) matches closely to the entry.

The parameters of electronic name clearance systems need to be set so that matches will occur with close matches rather than exact matches. For instance, with the use of names, applicants will

sometimes provide a middle name, middle initial or no middle name at all. If the database expects one form and one form only, either of the other two forms can miss hitting on the clearance system. Some fraud perpetrators have learned to vary name, birth date, national number, or other critical elements. It is also recommended to clear former names when names have been changed by court order, marriage, etc.

Transliteration from foreign languages and alphabets is a concern, and it is important to have high quality, reliable transliteration software. The use of name check algorithms that can identify characteristics of different languages and alphabets, and that are designed to check various types of names, will improve name check accuracy.

Resolution of a match (including voiding of verified matches) should take place as part of the entitlement/adjudication process. The issuance system should be built so that it records the name or identification number of the employee overriding a match, and some percentage of those overrides should be reviewed randomly by supervisory staff. All database checks should be completed and matches verified and cleared before the passport is released. For this reason the database checks should be done as early as possible in the process so as not to delay the release of the passport.

3.6 Travel Restrictions

The name, date and place of birth of each applicant should be checked against an electronic database containing the names of persons who are not entitled to a travel document for various reasons—for example, persons who have been involved in passport fraud in the past; persons wanted by law enforcement for criminal activity; persons who have failed to pay child support, etc. The data included in this database should come from various TDIA partners and stakeholders, such as border control and immigration authorities, law enforcement, correctional services, foreign affairs authorities, national security agencies, Interpol or other international sources, etc. Alternatively, if this information can be checked against partner databases it does not need to be added to the TDIA database. Facial recognition or other biometric comparisons can also be done against travel restriction databases containing photos or biometrics of known and flagged individuals. These databases must be updated regularly.

3.7 Action When Anomalies are Detected

If the TDIA detects any anomalies in the process of establishing identity (e.g. credentials or information remains unverified, or some kind of fraud is discovered), these anomalies should be investigated before continuing with the issuance process. Investigation should include the following procedures:

- Unless it is clear that it is a fraudulent matter (in which case the matter should be forwarded directly to dedicated investigations staff) an explanation should first be sought from the applicant. If the applicant's explanation is not satisfactory, then the application should be investigated further by dedicated investigations staff.
- If there is a legitimate discrepancy that requires amendment or replacement of the breeder or support documents, applicants should be referred back to the authority that issued these documents.
- Documents suspected to be fraudulent should be seized until the applicant's identity has been fully established.
- If the applicant's identity or credentials are proven to be fraudulent, details of the fraud should be recorded in a database(s) that can be searched during future applications to prevent further fraud using that identity or those credentials.

4 Treatment of Materials and Blank Books

4.1 Summary

Materials and blank travel documents include blank booklets, identification and observation labels as well as security laminates. The protection and secure management of blank travel documents and raw material is critical to the integrity of the production and issuance program because if they are lost or stolen, they can be used to create very persuasive counterfeit personalized documents.

The TDIA should have documented policies and procedures related to the treatment of materials and blank books. Information in this chapter can be used to develop policies and procedures. Compliance with the policy and procedures should be closely monitored.

4.2 Book Production

In many countries, the travel document book is produced by a private company or a third party in independent facilities. The TDIA should ensure that the blank materials are produced and stored in facilities that are secure, following best practices for Security and High Security Zones in Chapter 7. Security practices for shipping, storage, accounting and destruction must be as stringent for the blank materials used by the manufacturing organization as for the blank books used by the TDIA.

4.3 Numbering

Travel document blanks should be produced using a numbering system that allows individual documents to be identified at any step of the issuance process. This will facilitate accountability and tracking while travel documents are produced, shipped, stored, and personalized. It is strongly recommended that this number become the travel document number to ease the tracking of lost or stolen books. In other cases, the travel document accounting records (numbering) should be retained, at a minimum, for the period of validity of the document. The booklet/travel document number should appear on each internal page of the book (i.e. printed, laser perforated etc.), and each page should be numbered (1-2-3-4…) in sequence. Documents may also contain version numbers for ease of verification. Physical security techniques such as laser perforation, for the booklet number, and UV ink, for the page number, should also be used to mitigate the risk of the booklet being altered or some material being used to create a new document. Other security features can also be used.

4.4 Shipping and Storage

Materials and blank books should be contained in a highly secure repository, such as a vault or a safe, with access limited to trusted individuals having supervisory authority. Access to unique materials and blank book storage should be limited to the smallest number of persons possible. Access to the vault or safe should be controlled using ID cards, biometrics, pass codes, etc., and the facilities containing the material and blank books should be monitored 24/7 using security guards and/or CCTV. In addition, the secure area should include safeguards against fire or other catastrophic losses, and backup storage locations should exist to ensure continuity of operation in the case of the destruction of all blank books and materials (Chapter 7).

When travel document blanks and consumables are shipped from/by the manufacturing facilities to the TDIA, they should be transported in a secure manner (i.e. by armoured vehicle used to transfer cash and security officers/guards) Transportation should be closely monitored and all books and materials tracked and accounted for at all time. The transmitter and the receiver both have to sign off the batches of documents received.

Assigning blank books to production staff should be conducted by at least two employees (four eyes principle, dual signing). Books should be protected, even when assigned to production staff, and locked away securely whenever an employee absents himself or herself from their workstation, e.g. at breaks and lunch time. Unused blank books should be returned to the secure repository at the end of each day or each work shift period.

4.5 Accounting

The inventory control numbers put into the blank books when produced should be tracked from the time the blanks are shipped by the manufacturer and should continue to be tracked until each and every one has been accounted for either as a completed travel document or a spoiled book. The tracking records should be maintained throughout the validity period of the travel document. This involves counting and recording blank document totals, every time they change hands, by at least two employees.

Blank books should be counted out of the locked repository in the morning, and unused passports should be counted back in each night, or at the end of work shifts, by two individuals. The actual count of blank travel documents should be reconciled daily at the end of the day to make certain that the count of documents on hand matches what the automated inventory says. If the latter record is maintained by hand, reconciliation is still required. Records should be maintained for at least the validity period of the document. These records should be inspected daily, by a third party, or on a shift basis.

Staff members entrusted with travel document blanks, for access to storage or for production, should be checked every time they leave TDIA premises, or on an ad hoc/random basis, to ensure that no blank books have been removed.

4.6 Destruction

The actual destruction of spoiled, defective and excess blank books or partially completed travel documents should be conducted and witnessed by two responsible staff members (four eyes principle). Destruction of books should be done on a daily basis to avoid large numbers of books building up. These books should be accounted for to match the master inventory.

5 Personalization and Delivery

5.1 Summary

The personalization of a travel document refers to the variable data added to the blank booklet. In a passport it includes the applicant's personal data (including the bearer's photo) to be printed on the data page and the information to be encoded in the chip.

Once personalized, the travel document may be released to the applicant using various means: in-person pickup (or release to a third party); secure mail, delivery or courier services. Depending on the method(s) chosen, some techniques can be used to mitigate the risk of the travel document being released to a person impersonating the true applicant or using a false identity.

5.2 Personalization

The personalization function must be carried out in a highly secure area such as a vault where only select individuals have access. Access control to the vault can be secured by various technologies and means such as ID Cards, Biometrics, etc. More details on physical security can be found in Chapter 7.

As the personalization process requires the manipulation of blanks and material, all best practices included in Chapter 4 should be followed, including the presence of two persons at all times during the personalization process. The transmission of the applicant's personal data to the printer/encoder must also be protected by IT security best practices as specified in Chapter 8.

5.2.1 Quality Control

Once personalized, the travel document must be subject to a quality assurance process to ensure that it contains no mistakes or imperfections that may have an impact on the scrutiny the holder would be subject to by border officials when travelling.

For a regular MRTD, the MRZ should be read by a reader equivalent to those used at the border and the MRZ information should be compared to the data page, the applicant information contained in the TDIA database, and the original forms submitted by the applicant. The data page should also be reviewed for proper finish, stitching and lamination and a few designated security features verified (randomly).

For an eMRTD, the data on the chip (including the photo) should also be read by a reader and compared to the data in the travel document, the MRZ, the TDIA database and the applicant forms. The validity/integrity of the Digital Signature used to protect the chip should also be verified.

5.3 Delivery

5.3.1 In Person Pickup

It is suggested that the applicant pick up his or her own newly-issued travel document. However, this is not always geographically practical. It could also result in a high volume of applicants coming into the office. If in person pickup is used, a pickup receipt can be provided to the applicant at the time of the application entry.

When releasing the travel document, the employee should verify and compare the photo in the travel document (including in the chip) to the photo in the database and to the applicant (live person). To certify that the person picking up the passport is the rightful holder, additional

techniques can be used. The applicant may be asked to show an additional ID bearing a photo or personal questions such as address, mother's maiden name, etc. Biometrics, i.e. facial recognition technology or fingerprints, could also be verified. A receipt should be signed by the applicant stating that the travel document has been picked up on a specified date and time, and the Pickup Status should be identified in the TDIA database.

It is not recommended that the travel document be released to a third party such as an agent or relative. However, if it is permitted, written authorization should be provided and the identity of the person should be established using ID documents bearing a photo. A receipt should be signed by the person picking up the travel document.

The TDIA could use an alert system that monitors if standard time periods have been passed once the travel document is ready for pickup. If, after a period of time, documents are unclaimed the applicant should be contacted. Cases of unclaimed travel documents should be investigated for fraud.

5.3.2 Mail Services

If personalized travel documents are delivered by mail to the applicant, reliable mail service is necessary. If public mail service is unreliable, an alternative controlled mail or a private delivery service, e.g. a courier service, could be used. In all cases, a signature of receipt by the applicant or someone living at the same address should be required upon receipt of the travel document. A confirmation of the delivery should also be indicated in the TDIA database. If the mailing service used does not require a signature upon receipt, other means could be used to confirm receipt of the travel document: return of a code word or return of a receipt to the TDIA. Again, the TDIA could use an alert system to monitor the confirmation of receipt of the travel document in standard time periods.

Reasons for travel documents mailed out and not received by the applicant include:

- travel document mailed to wrong address due to the TDIA error;
- travel document lost in mail due to mail or courier service error;
- travel document mailed to wrong address due to applicant error; or
- may be an indicator of fraud.

The fact that a correctly addressed travel document comes back to the issuing authority as undeliverable may be a fraud indicator, and should be checked against the information contained in the application form. If the address is correct and verified as existing, the applicant should be contacted to come in and pick up the travel document. Otherwise the file should be referred to fraud investigators.

If an applicant reports that he has not received a travel document that the TDIA has sent, the case should be handled in the same way as lost or stolen travel documents. The document should be immediately declared invalid and put into a lost/stolen passports database. The applicant must be advised that if the travel document is subsequently found or received the applicant should not use the travel document. It should be returned to the TDIA for secure destruction.

6 Document Security

6.1 Summary

This chapter refers to the physical features, techniques, and characteristics of travel documents including strengthening their security and improving their resistance to attack and misuse. With widespread access to low cost technologies including high quality scanning, colour copying, image processing and photo quality printing, the capacity of individuals to produce convincing counterfeit travel documents and very deceptive alterations has increased exponentially. The following are physical threats to travel documents:

- counterfeiting of a complete passport or travel document;
- photo-substitution;
- deletion/alteration of text in the visual or machine readable zone of the MRTD data page;
- construction of a fraudulent document, or parts thereof, using materials from legitimate documents;
- removal and substitution of entire page(s) or visas;
- deletion of entries on visa pages and the observations page;
- theft and personalization of genuine document blanks; and
- tampering of the chip (where present) either physically or electronically.

An overview of the main developments in MRTD technology and security concepts is provided in the present document. Document Security is discussed in detail in the **Informative Annex of Document 9303 Volume 1 Section III: Security Standards for Machine Readable Travel Documents**.

6.2 Machine Readable Travel Documents (MRTD)

The MRTD is a travel document containing, in a standard format, the holder's identification details, including a photo (or digital image), with mandatory identity elements reflected in a two-line machine-readable zone (MRZ) printed in optical character recognition format. The ICAO MRTD specifications are included in **ICAO Document 9303 Part 1, Volume 1**.

This type of travel document has been developed to enhance both international interoperability and security. It represents major benefits to all stakeholders including governments, airlines and travellers, at relatively low implementation costs. The uniform layout of the document improves the capacity for visual authentication. The standardized data that can be read by readers enables linkage to various databases and sharing of the information with several stakeholders to better detect false, stolen or fraudulent travel documents and consequently improves border control processes. MRTDs also simplify the use of Advance Passenger Information (API) systems.

MRTDs enable automated data entry, a significant improvement over manual data entry. Faster data entry with fewer errors is an example of the facilitation benefits brought by MRTDs. Gains in facilitation, global interoperability and security brought by MRTDs led to the adoption of **ICAO Standard 3.10** requiring all ICAO Member States to start issuing only Machine Readable Passports (MRPs) by April 1, 2010 and to gradually remove non-Machine Readable Passports still in circulation by November 24, 2015.

The Implementation and Capacity Building Working Group (ICBWG) was established to assist the ICAO Secretariat in performing capacity building outreach activities to help countries meet the 2010 deadline. It is recommended that countries that need help to implement their Machine Readable Passports program contact the ICAO Secretariat MRTD Program.

6.3 Electronic Machine Readable Travel Documents (eMRTD)

The work of ICAO since 1998 has led to the development of a new generation of travel documents: the eMRTD. The eMRTD is an MRTD containing a contactless integrated circuit (IC) chip within which is stored data from the travel document data page and a biometric measure of the passport holder. The data encoded in the chip is protected by Public Key Infrastructure (PKI) cryptographic technology. The ICAO eMRTD specifications are included in **ICAO Document 9303 Part 1, Volume 2.** While ICAO identified the facial image as the biometric of choice to achieve global interoperability, fingerprints and iris can also be used as secondary biometrics. Basic Access Control (BAC) or Extended Access Control (EAC) are used to protect data against unauthorized access.

The eMRTD represents the greatest improvement in travel document security since the introduction of MRTDs. It improves the integrity of travel documents by providing the ability to match the information contained in the chip to the data printed in the document and to the physical characteristics of the holder, i.e. three-way verification. The eMRTD also enables machine assisted verification of biometric and biographical information matching both the traveller to the document as the rightful holder and also checking simultaneously against appropriate watch lists or databases.

Although the eMRTD is not the answer to all document fraud, it offers greater protection against fraudulent misuse and tampering. It also reduces the risk of identity fraud at border crossing through improved detection of impostors.

ICAO Recommended Practice 3.9 of the Chicago Convention Annex 9 is for ICAO Contracting States to incorporate biometric data in their machine readable passports, visas and other official travel documents

⇒ For more information on the ePassport: APEC, a Guide to Biometric Technology in MRTDs (http://www.apec.org/apec/publications/free_downloads/2007.html)

ICAO Public Key Directory (PKD)

An additional layer of security is added when the authenticity of the data on the eMRTD chip is validated at the border using Public Key Infrastructure (PKI) certificates. Validation of eMRTD is done to confirm that:

- the document held by the traveller was issued by a bona fide authority;
- the biographical and biometric information endorsed in the document at issuance has not subsequently been altered.

The PKD was established by ICAO to act as a central broker to manage the exchange of ePassport public key infrastructure certificates and certificate revocation lists. This central role is critical to minimizing the volume of certificates being exchanged between countries, to ensure timely uploads and to manage adherence to technical standards to ensure interoperability is achieved and maintained.

In April, 2009 ICAO Council adopted a Recommended Practice related to the ICAO/PKD. (see section 6.4.2 on ICAO Standards and Recommended Practices.)

⇒ For more information on the PKD and how to become a member: http://www2.icao.int/en/MRTD/Pages/icaoPKD.aspx

6.4 ICAO Standards, Recommended Practices and Specifications

6.4.1 Document 9303 Specifications

To meet global interoperability and therefore enhance security, travel documents must be compliant with the specifications of the appropriate part of Document 9303:

Part 1: Machine Readable Passports

> **Volume 1—**Passports with Machine Readable Data Stored in Optical Character Recognition Format
>
> **Volume 2—**Specifications for Electronically Enabled Passports with Biometric Identification Capabilities

Part 2: Machine Readable Visas

Part 3: Machine Readable Official Travel Documents

> **Volume 1—** Machine Readable Official Travel Documents - MTRDs with Machine Readable Data Stored in Optical Character Recognition Format
>
> **Volume 2—** Machine Readable Official Travel Documents -Specifications for Electronically Enabled MRTDs with Biometric Identification Capabilities

To order *Document 9303:* http://icaodsu.openface.ca/mainpage.ch2 .

Historically, Document 9303 has not made recommendations specific to the security features to include in the travel document. Each state should decide, based on risk assessments, which combination of security features meet its security needs.

However, because of the need for increased document security, ICAO has published a guidance document on **Security Standards for Machine Readable Travel Documents** as an **Informative Annex of Document 9303 Volume 1 Section III.** The recommendations included in this document cover the security of the materials used in the document's construction, the security printing and copy protection techniques to be employed, and the processes used in the production of document blanks. The use of a good combination of these features and techniques, incorporated at the time of production and/or at the time of document personalization, is recommended to address different forms of potential attacks to the document. The TDIA should ultimately lead, and be the approval authority for, the design of the travel document, the security features, and the selection of materials used in it.

6.4.2 ICAO Standards and Recommended Practices

Some Standards and Recommended Practices included in Chapter 3 of the Annex 9 of the Chicago Convention specifically concern travel document security. TDIA must comply with these Standards and follow, to the extent possible, the Recommended Practices.

Document Security
Standard 3.8 - Contracting States shall establish controls on the creation and issuance of travel documents in order to safeguard against the theft of their stocks and the misappropriation of newly issued travel documents.

Standard 3.7 — Contracting States shall regularly update security features in new versions of their travel documents, to guard against their misuse and to facilitate detection of cases where such documents have been unlawfully altered, replicated or issued.

Because security features in a secure document can be compromised at any time after implementation, it is a good security practice to change the design/security features approximately every five years. Periodic introduction of redesigned and more secure versions of travel documents will impede forgers and counterfeiters. More advanced and secure technologies should be incorporated in each new version of the travel document and must be communicated securely and in confidence to all officials required to examine the document. In order to facilitate this, travel documents should indicate under which version they were issued.

Passport Validity Period
Standard 3.4 — Contracting States shall not extend the validity of their machine-readable travel document.

Recommended Practice 3.16 - …Contracting States should normally provide that such passports be valid for a period of at least five years…Note 1 — In consideration of the limited durability of documents and the changing appearance of the passport holder over time, a validity period of not more than ten years is recommended.

Studies demonstrate that the security features in a secure document begin to be significantly compromised within a few years after implementation. Redesign and replacement of the document is therefore recommended after five years. However, service, volume and financial implications are all important elements to be taken into consideration in the determination of the passport validity period.

One passport/One person
Standard 3.15 - Contracting States shall issue a separate passport to each person, regardless of age.

In 2002, ICAO adopted the one passport/one person standard to maximize the benefits brought by machine readable passports and to combat international child trafficking and abduction.

Machine Readable Passports
Standard 3.10 — Contracting States shall begin issuing only Machine Readable Passports in accordance with the specifications of Doc 9303, Part 1, no later than April 2010.

Standard 3.10.1 - For Passports issued after 24 November 2005 and which are not machine readable, Contracting States shall ensure the expiration date falls before 24 November 2015.

Biometric Travel Documents
Recommended Practice 3.9 - Contracting States should incorporate biometric data in their machine readable passports, visas and other official travel documents, using one or more optional data storage technologies to supplement the machine readable zone, as specified in Doc 9303…

ICAO Public Key Directory
Recommended Practice 3.9.1 - Contracting States (a) issuing or intending to issue ePassports and/or (b) implementing at border controls automated checks on ePassports should join the ICAO Public Key Directory (PKD).

6.5 Types of Travel Documents

It is highly recommended that minimum security features (referred to in Section 6.4.1 – Doc 9303) be added to all types of travel documents, including diplomatic, official, special, and especially temporary and emergency passports. Diplomatic and official (special) passports should use the same blank books and materials (except book cover colour) as regular passports.

Temporary and/or emergency passports are issued overseas for urgent, proven travel situations or residency requirements. The validity of an emergency or temporary passport is limited to meet the applicant's submitted travel requirements. In many cases, this is a single trip to return to the home country. It is recommended that these documents, which currently constitute high security risks, include some minimum security features in order to avoid deletion or alteration of data.

7 Facility Security

7.1 Summary

Facility (or physical) security includes the means used to prevent unauthorized access to facilities and restricted zones by external or internal individuals and to protect assets and information. Multiple strategies and technologies exist to secure facilities. The TDIA should use a variety of these as deemed appropriate considering threats and vulnerabilities as well as costs, privacy and inconvenience on operations.

7.2 Physical Security Policies

There should be a comprehensive physical security policy in place covering all facilities and spaces used for the issuance process including office spaces, production areas, customer services areas, network and computer rooms, etc. This policy should follow the country governmental standards and guidelines as well as internationally acceptable standards.

Although primarily an ISO information technology standard, ISO/IEC 27002:2005 - Information Technology -- Security Techniques -- Code of Practice for Information Security Management is an ideal reference to improve the security of managing information in organizations. The standard provides recommended best practices related to, among other things, physical and environmental security. It provides safeguards and countermeasures on the mitigation of security risks as well as appropriate implementation assistance related to physical entry control, securing of rooms and facilities, working in a secure area, public access, and delivery and loading areas, all of which are applicable to TDIA facilities.

ISO 27007 is closely linked to ISO/IEC 27001:2005, which provides the procedures and guidelines for developing, implementing and maintaining an Information Security Management System (ISMS). Both standards are available at http://www.iso.org/iso/store.htm.

It is recommended that all TDIA facilities, or at least the operation, security and high security zones (see table below), be owned by the government to ensure complete control and flexibility for the installation of physical security measures. Facilities of public and private partners involved in the issuance process should also meet the security standards defined by the TDIA.

All employees should be briefed and trained on the physical security policies and practices. There should be sanctions for staff who do not follow them, e.g. when they do not escort visitors; do not wear their badges; give access to unauthorized personnel in restricted zones, etc.

- For an example of a governmental security policy: the Canadian Government “Operational Security Standard on Physical Security “, (2004): http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/osps-nosm-eng.asp.

7.3 Security Zones

All TDIA facilities and work areas should be defined in terms of security zones to which physical security protection must be adapted based on the activities undertaken in these places, the value of assets and the data stored:

Zones	Activities/Functions	Physical Security
Non-restricted-access area		
Public Zone	• Surrounding the facilities	• No access control

	• Escalators	• May be monitored to detect suspicious activities
Reception Zone	• Customer service area • Initial contact between visitors and organization	• Access limited to specific time of day • Intrusion detection • Monitored at entry points (security personnel) • Monitored for work-related violence • May have other physical security protection to protect employees
Restricted access areas		
Operation Zone	• Office space • Handling of application/entitlement	• Access controlled • Intrusion detection • Monitored • Locked cabinet and safe (for work in progress/data)
Security and High Security Zones	• Personalization of travel documents • Storage of blanks • Cash handling area • Network room • Storage of applicant files/archives	• Access controlled and highly restricted • Intrusion detection • Monitored 24/7 • Special physical security specifications, e.g. vault, safe.

7.3.1 Customer Service area

Physical security is necessary to ensure the health and safety of employees at work against work-related violence. Due to the nature of travel document production and issuance, it is possible that situations may arise where employees are under threat of violence because of their duties or because of situations to which they are exposed.

The area where the public applies for and receives travel documents should be built so that customers cannot have easy physical access to the fees paid or to staff, for the safety of the staff and the security of blank books and materials. If required, physical security may include duress alarms, bullet-proof glass or magnetometers or other screening technology to detect weapons carried by applicants. It is also recommended that security personnel be present during working hours to provide a calming presence in cases where applicants become agitated and to escort applicants out of the area should they become disruptive.

There may also be a secure interview room where law enforcement agents can interview possible fraud perpetrators who are caught during the application process or when they come back to pick up a travel document. It may, however, be preferable in certain circumstances for law enforcement personnel to remove the person from the premises for questioning.

7.3.2 Handling of applications and entitlement function (Operation Zone)

Operations, security and high-security zones should be designated as a Restricted Area and access should be for authorized personnel only and not for all employees. The access to application handling offices must be controlled and limited to those who are authorized as per their functions and who have undergone a screening process to the appropriate security level. At times, visitors or contractors may have duties in a Restricted Area but they should be escorted at all times. Cleaning staff and security guards must also be security cleared. Employee access to this area should also be restricted to certain time periods, i.e. during their work shift only.

7.3.3 Personalization area (Security and High Security Zones)

This area includes a vault (safe) area where blank books and material are stored and where travel documents are personalized. Access to this area should be highly restricted using various access control means. The use of a two-factor authentication such as electronic cards, keys, PIN and biometrics is recommended. The area where travel document personalization occurs must be placed under secure lock down at the end of every business day. Monitoring systems and intrusion detection devices should be employed to minimize the chance of theft. In order to prevent internal theft, a policy should be in place that prevents employees from being alone in secure areas. As a plot involving more than one person is inevitably more complex and requires advanced planning, the opportunity for spontaneous crime is reduced (Chapters 4 and 5).

7.4 Access Control and Monitoring

Control of access is an important component of any physical security approach. Of course, whether or not controlling access is effective in discouraging a threat depends on the nature of the threat. Access control will provide minimal protection from those who already have access to the facilities and therefore internal controls such as those exposed in Chapter 9 should be in place. Monitoring and intrusion detection equipment will be useful to remotely survey entry areas where people can gain access to the facilities and some zones that necessitate higher security.

There are a variety of methods to control access, intrusion detection and monitoring, each of them providing different levels of protection, at different costs. A combination of strategies and technologies should be used. Consideration should be given to the level of inconvenience that each option provides and the impact on the privacy of employees and the public. Access control should be as convenient to normal operations as possible. Below are some strategies that could be employed in all TDIA facilities, based on the security level required and threat risk assessments:

- **Security personnel**: Guards who have the task of providing on-site security and monitoring for all facilities 24-hours a day, seven days a week.

- **Access identification badges**: Are to be worn at all times by employees while in restricted zones (operation, security and high security zones). These badges should display clear photos of the holder and have colour or other obvious codes to visually indicate the access privileges of the holder. Access rights for all staff should be routinely audited. If employment is terminated, the access badge must be reclaimed by the organization. Visitors and contractors should be given temporary badges in exchange for a piece of acceptable photo identification which will be retained by security personnel. Staff members are to sign in visitors and the piece of identification will only be returned once the visitor access badge is returned.

- **Escorts**: Visitors should be escorted at all times by a staff member when in restricted zones. This also applies to TDIA employees which security clearance or position does not give access to some zones.

- **Electronic or physical barriers at entry points**: Such as doors, turnstiles, gates.

- **Locks**: Use limited-distribution keys, pin numbers, electronic cards or keys, or biometrics. Pin numbers should be changed on a regular basis. Even during working hours, the exterior doors to restricted zones should remain locked. Only government employees should have keys, combinations or use electronic cards having access. Others needing entry should be monitored and admitted using visual-recognition door monitors and a remote door-release mechanism.

- **Intrusion detection**: Such as alarms and motion sensors.

- **Monitoring**: Using door monitors, cameras and CCTV. The records of monitoring video should be kept for appropriate periods or more than three months.

7.5 Other Physical Security Protection and Practices

Some areas or zones require specific security measures. Security and High Security Zones for example require special physical construction such as a vault or safe. Customer services area may demand screening equipment to detect weapons and employee protection systems including bullet-proof glass and duress alarm.

Mail, including travel document application and materials received should be screened in an appropriately located mailroom. Mailroom staff should be trained to screen for suspicious materials using X-Ray or other methods and to initiate a protocol once a suspicious package has been identified.

Protection of facilities, assets and data against fire and other catastrophic losses should also be considered. Arrangements for alternative sites and backup storage sites should be in place to ensure the continuity of operations in case the issuing facilities are not accessible or in case of destruction of materials or data.

Organizational information and applicant personnel data must be protected. The use of safe, locked cabinet and protected rooms is required to store and protect information. Destruction or shredding devices are also to be used to eliminate information that is no longer required. This is discussed in Chapter 2.

8 Information Technology Security

8.1 Summary

Information Technology (IT) security is defined as safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information. In the past it was possible to protect information by simply controlling physical access to that information. In our modern networked age this is more of a challenge as a vast quantity of private information is stored on computer system networks that are often interconnected.

This is a concern for the TDIA, which has become more and more automated and is using information technology to improve efficiency, security and service delivery. At the same time, the number and potential severity of threats, vulnerabilities and incidents are similarly increasing. Because TDIA demands the collection of detailed personal information, sometimes including biometrics, the protection and security of IT systems and databases is crucial.

8.2 IT Security Policies and Practices

There should be a comprehensive IT Security Policy in place up-to-date with current technologies and practices, covering all IT systems, databases, information flow, etc. This policy should refer to, and incorporate current international standards such as the ISO/IEC 27002:2005 Standard-Information technology -- Security techniques -- Code of practice for information security management: http://www.iso.org/iso/store.htm. (Referred to in Chapter 7).

This ISO standard provides a guideline for developing appropriate security standards and security management practices regarding all forms of information. Security policies and practises are a central element of this standard which covers the complete range of security management. It is divided in eleven management areas from security policy management to business continuity management.

An important element of the standard is the assessments to identify risks and protection requirements. This includes vulnerability assessments, IT data privacy assessments, loss of database information, unauthorized data access and any other related assessments which should be performed regularly to implement security protection, prevention and mitigation measures.

The IT security policies and practices should deal with:

- appropriate **confidentiality** classifications of databases and related information such as watch lists, biometrics, and other information assets. Means and technologies should be in place to prevent this information from being accessed, intercepted, or otherwise copied and obtained electronically by the wrong persons.
- appropriate **data integrity protection** of databases and related information preventing this information from being changed, added to, or deleted except in the properly defined processes.
- appropriate **data availability** of databases and related information preventing this information from being blocked or hidden from legitimate users when it is required.
- appropriate **permissions of access** to databases and related information such that this information can only be accessed by **the authorized intended users** of the information.

All these policies, practices, technologies and methodologies should have been evaluated by professional IT auditors to verify their efficiency and their performance.

All technology products such as database software packages, servers, communications facilities, hardware security modules, and other commercial products that are used, should be certified at the appropriate Evaluation Assurance Level (EAL) security level. The cryptography devices used should have been certified to the appropriate level using international standards such as FIPS 140-2 or equivalent.

8.3 User Security

8.3.1 Access control

Access to the TDIA IT system and databases must be restricted. The equipment should be limited by means of biometric identification or unique username and passwords that allow an authorized employee to log on to the system. All individuals should be limited by access and processing permissions to certain databases, applications and tasks. Passwords used should be random number and letter combinations that can't be guessed. Birthdays, parent's names, etc. should not be used as these may be commonly known. Logons and passwords should be forced by the system to be changed regularly. All sign-on sessions should automatically terminate after short periods of inactivity and automatically require the user to re-enter the password to logon. Employee access rights should be audited on a regular basis and IT accounts for persons who are no longer employed by the TDIA should be cancelled immediately. The system should prevent access outside of normal working hours without supervisor override.

The equipment should have a monitoring and audit trail mechanism to indicate who has accessed the system and which information was consulted. Computer records of logon and usage should be maintained for a reasonable time. These records should be reviewed by management personnel to identify irregularities in computer access and wrongful access should be subject to specific penalties. This is even more important for VIP files. The organization must inform and regularly remind personnel of their IT security responsibilities and provide training. In the case of an IT security incident, an investigation should be performed and sanctions imposed if it is found that there has been misconduct or negligence.

8.3.2 Internet and email use

Internet access should be denied to staff or contractors from any computer or terminal used in the travel document issuance process. Such devices should be physically and technologically segregated: either used for travel document application processing or for inter and intra-office email or Internet.

There should be a program in place to randomly but regularly monitor email messages and Internet application accesses by all employees and contractors, in order to detect matters or communications which may be of concern. This process should be very well protected by internal and strict privacy policies and practices, such that innocuous personal information learned from the monitoring is never released for any reason. All information resulting from monitoring that is not of security interest should be regularly purged from records.

8.4 IT Personnel

IT personnel should have special access rights for entry to IT facilities, such as computer equipment rooms, physical databases and networks, communications facilities and back-up locations. These access privileges should involve two-factor identification and always require two or more authorized individuals at any time.

All responsibilities related to an IT system should not be given to a single individual as it would make the system vulnerable to undetected abuse. Responsibilities should be segregated and clearly defined. The IT infrastructure should be set up such that no one individual, regardless of

seniority, ever has the right to overrule security policies and practices, make arbitrary decisions, take arbitrary backup of databases and other information files, or in any way compromise the issuance system and its confidential information.

The IT personnel should be regularly reminded of security policies. Review and audits should be performed regularly and sanctions imposed if it is found that there has been misconduct or negligence.

9 Protecting and Promoting Personnel and Agency Integrity

9.1 Summary

To deliver its services to the population, the TDIA is dependent on and vulnerable to the actions, accuracy and decisions of its staff. Therefore, having trustworthy, capable, and operationally safe employees is of vital importance. Authenticity of travel documents is dependent on the integrity of the people who issue them, and an effective personnel security program is necessary to ensure that the issuing process is conducted with the utmost integrity.

Staff morale, work organization and internal controls have a great impact on the prevention and detection of internal fraud. If fraud is suspected or detected, mechanisms need to be in place to proceed with internal investigations and possible sanctions.

The Western Australia Corruption and Crime Commission's "Misconduct Resistance Integration Guide" is a useful reference: http://www.ccc.wa.gov.au/pdfs/CCC-MR-GUIDE.pdf.

9.2 Security Clearances and Security Briefings

9.2.1 Background and Reliability Screening

The TDIA must ensure that individuals having access to the issuing facilities and systems are reliable and trustworthy. This starts even before employees are hired by the organization by verifying that the individual considered for employment is dependable and not easily corrupted. Before employees are offered a job, it is important to execute background and reliability checks. Contractors should also undergo these checks. The extent of the screening should be related to the position, responsibilities, the access, and the level of decision-making the employee will have. All staff positions should be assigned a security level classification that recognizes the sensitivity of the position and the employee occupying the position must have successfully obtained a security clearance to that level.

Checks should be made in collaboration with law enforcement, police or national security agencies. For positions with higher security level classifications such as managerial functions and those involving decisions on entitlement to a travel document, the checks should be more thorough and may include family, friends and previous employer interviews, as well as a review of financial history (to minimize the risk of financial vulnerabilities). It is recommended that entitlement officers be citizens of the country.

Culture and tradition should always be examined to ensure it does not overrule or circumvent the probity of performing background and reliability checks, or the hiring of any individual.

9.2.2 Regular Security Checks and Constant Vigilance

Employee's incurring unmanageable debt can make them vulnerable to bribery or corruption. Greed is merely one motivator for employees to commit fraud, and evident signs of living above their means should be taken seriously. Managers must remain vigilant once a security clearance is granted, and act on any new information that could put into question an individual's reliability or loyalty. Security checks on employees should be redone regularly on a prescribed schedule during the period of employment. Although there is no definite mechanism to assess the potential of an existing employee for malfeasance, periodic background checks can highlight some security risks.

9.2.3 Barriers to opportunistic risks

Another threat to keep in mind is that employees with no known criminal record or other cause for suspicion may easily pass regular security clearances, but this does not guarantee that they will remain dependable. Employees may be subject to various external pressures to commit fraud and therefore special care must be taken to limit opportunistic risks and to ensure the continued reliability and loyalty of individuals. Delimitation of secure areas and internal controls to limit the authority of employees, both physically and electronically, must be in place in order to discourage and uncover staff malfeasance. This also applies to any partner organization involved in the production and issuance of travel and identity documents. It is important to note that a security clearance does not in itself confer a right of access to secure information or areas. Even security cleared individuals should not be allowed access to an area or data unless their duties require such access. Limiting which employees are authorized to access secure areas will reduce opportunistic risk.

9.2.4 Temporary Staff

Many TDIAs employ temporary staff during peak periods. This can be a major security threat if they are not screened properly due to time constraints. It is therefore crucial that temporary staff undergo the same background checks as permanent employees. A pool of pre-cleared staff should be maintained by the TDIA to use in case of overload or understaffed situations (Refer to Chapter 1).

9.2.5 Security Awareness and Codes of Conduct

Once a new employee or contractor reports for duty with the issuing authority he should be given oral security instruction and written guidelines on the issuance authority's internal controls and security policies. Individuals must be briefed on their access privileges and prohibitions attached to their security clearance level. The employee, starting on his or her first day and for the duration of employment, should receive regular security briefs and training to maintain his or her security awareness (Chapter 1).

At the beginning of his or her employment, employees should also be introduced to the organizational standards of conduct or values and ethics guidelines. These guidelines communicate the actions and comportments that are viewed acceptable or unacceptable by the organization. They also include specific conflict of interest clauses, prohibiting the acceptance by staff of gifts and gratuities from vendors and suppliers doing business or seeking to do business with the issuing authority and a similar ban on accepting gifts and gratuities from travel document applicants for performing normal tasks or in expectation of special favours. Time should be provided so that the employee can read the guidelines and ask questions. Managers should ensure employees understand and ask him or her to sign an acknowledgement of receipt and understanding.

9.3 Work Organization

9.3.1 Segregation of Tasks

Prescribed job functions should be established such that one employee cannot perform all the travel document entitlement and issuance functions. This means that it would require several employees to issue a travel document to someone who tries to buy or obtain one through subversion. Since it is harder to arrange a conspiracy to commit malfeasance than for one person to do so alone, it is far more likely that the TDIA will uncover conspiracies involving multiple employees than single malfeasants acting alone.

9.3.2 Random Delegation of Work

In order to reduce the possibility of internal malfeasance, it is recommended that office flow procedures prevent the possibility of the public being able to select the employee they wish to deal with. For example, where more than one employee is accepting travel document applications from the public, the flow of applicants should be done in such a way that all counter stations feed from a single line according to who is free to take the next application (rather than applicants self-selecting a particular employee by standing in a specific line).

The same principle applies with desk entitlement. Staff should be required to take the next batch of work in sequence. This reduces the possibility of staff members being able to access or deal with specific applications. For the same reason, staff should be required to rotate through several functions, e.g. dealing with the public; desk entitlement of mailed applications; data entry; verification of breeder documents, etc.

Staff and management must not process or approve applications of acquaintances, friends and family. Only in exceptional circumstances should there be a method of expediting applications, e.g. VIPs. This exceptional service should be thoroughly documented and overseen by a nominated senior official who may not act alone in the issuance of any document.

9.3.3 Transparency of the process

Transparency is crucial for all steps of the issuance process. It is essential to log all vital decisions made during the issuance process, even more during important workload backlogs. Adequate notations in application files and databases regarding evidence seen and/or actions taken should be present to justify all the decisions taken by the entitlement staff. This provides adequate written justifications so that actions taken may be reviewed later during random audits, or if there is a specific question about why a decision was made on a given application. Clearly prescribed procedures for annotations should be part of a training program.

9.4 Staff Morale [Job Satisfaction]

The TDIA is well advised to pay attention to employee morale issues. Employees with high morale feel valued for their contributions, are more productive and effective in their jobs, and feel loyalty to the organization. In opposition, unhappy employees may become vulnerable and may be at greater risk of responding positively should they be approached to participate in malfeasance.

The most effective anti-malfeasance device available is to build a sense of self-respect and pride among employees in the accomplishments of the organization. Job satisfaction is one of the most important factors in ensuring that an employee remains loyal. Several elements influence morale and job satisfaction:

- a written job contract;
- a regular (or guaranteed) pay;
- fairness of pay;
- reasonable working conditions;
- a conflict-free environment;
- good supervision, management and communications;
- involvement in decisions;
- training and experience opportunities to qualify for higher graded work;
- good leave and other benefits of employment;
- possibility to file grievances and have these grievances fairly heard and dealt with;
- etc.

These are best managerial practices for any organization but are even more important for organizations whose mandate and work may impact national and international security. The time and expense involved in training supervisors and managers to develop the competencies of good leadership and good managerial practices is a worthwhile investment that cannot be overemphasized. Skilled managers are able to both improve productivity and deter employees from participating in internal fraud.

The organizational climate must reflect that the employer really cares about staff and their work. Employee recognition systems play a large part in this and everything from simply ensuring staff is thanked for their efforts; organizational and public appreciation; awards; or paid time off from work should be used to reward and recognize an employee's performance.

A good practice for senior management to measure employee morale and reveal problematic areas is to conduct and analyze the results of regular satisfaction surveys. This gives the opportunity for employees to express, in a confidential manner, their satisfaction with their work and with the management practices of the organization.

9.5 Internal Investigations and Sanctions

9.5.1 Reporting Security Incidents

Employees should be regularly reminded of the importance of being on guard and attentive to employee malfeasance and internal fraud including theft of documents, consumables and cash. Employees should be required to report all incidents and threats. Employees should also be encouraged to advise management when they are approached by persons wanting them to commit fraud.

The TDIA should have a documented policy related to security incident reporting which requires that all incidents, especially as they relate to misconduct and negligence, be reported. The policy should also outline the employee and management responsibilities related to the handling of the reports. Procedures related to incident reporting should reflect the requirement to have all incidents documented. They should contain clear direction on how the reports are to be handled including guidance on the appropriate investigating agency or TDIA unit, separate from operations, to which they should be referred. Depending on the nature and severity of the incident, investigations may be administrative or criminal. Reports should be confidential and the reporting employee should be protected against negative feedback regardless of the nature of the violation or the individual involved.

Through effective reporting and investigation of security incidents, vulnerabilities can be determined and the risk of future occurrence reduced.

9.5.2 Investigations

It should be clear, through strong legislation, which governmental agency has responsibility for investigating travel document fraud. Often, the responsibility will be split, with one agency having responsibility for external fraud and a different agency handling internal fraud. Regardless, it is important for the TDIA director to meet regularly with the leadership of those responsible for fraud investigations, both to be informed about cases in process and to make sure that the issuance authority is cooperating fully.

The findings of internal fraud investigators should be conveyed fully to the issuing authority, including the nature of the fraud, how it was committed, and what improvements could be made to prevent such instances from occurring in the future. This is important because the TDIA should

learn lessons from every instance of internal fraud, and should take rapid corrective action to prevent a reoccurrence.

9.5.3 Sanctions

The issuing authority must make sure that there are adequate laws to bring charges and prosecute employees suspected of internal fraud and that the laws provide for meaningful penalties. Sanctions should also be given in response to security incidents when there has been misconduct or negligence.

Persons whom investigators have determined are responsible for committing internal fraud should normally be dismissed with loss of benefits. This applies to minor as well as major incidences. By committing an act of fraud, no matter how slight, an employee has shown a willingness to break the rules. If warranted, they should be prosecuted to the fullest extent of the law, including criminal prosecution.

The issuing authority should press for significant penalties not only for the punishment involved, but even more importantly, as a deterrent—a proof to other employees that involvement in internal fraud will not be tolerated and that there are real penalties. The results of every case (conviction, dismissal, or resignation) should be publicized so employees who may have felt betrayed by their former colleague will know that the person was suitably punished.

10 Lost and Stolen Travel Documents

10.1 Summary

Misuse of genuine travel documents obtained in unlawful circumstances creates serious national security risks that must be addressed. Whether altered or left intact and used by an impostor, these documents can, if undetected, enable terrorists, criminals and irregular migrants to travel virtually unidentified.

Despite best security efforts, every country has experienced losses and theft of its travel documents either on an individual or multiple document basis. These travel documents may be blank books or fully personalized documents. The net effect is that there are potentially a high number of lost, stolen or cancelled travel documents currently in circulation being used by people other than the genuine holder. In some cases travel documents are reported lost or stolen but continue to be used by the rightful holder upon finding the document.

Preventive measures can reduce the number of lost and stolen travel documents and, once documents have been reported lost or stolen, mitigation measures can reduce the security risk the documents pose.

10.2 Preventive Measures

Preventive measures to limit incidences of travel document loss or theft include: public awareness to encourage document holders to take good care of travel documents; immediately reporting a missing travel document; and, more rigorous screening for applicants who have a history of lost or stolen travel documents.

10.2.1 Public Awareness

10.2.1..1 Safekeeping of the travel document

The TDIA should develop and establish a communication strategy to reduce incidences of theft by encouraging holders to securely store their travel document at all times. Public awareness campaigns educate travel document holders about things like how difficult and expensive it will be to obtain a replacement passport. Issuing authorities should ensure that the public is fully informed of their responsibilities in respect of the document they hold, and the possible consequences of loss or theft of the document.

10.2.1..2 Reporting of lost or stolen travel document

Public awareness strategies should be used to inform and encourage the public to take action should their document become lost or stolen. The public should report a lost or stolen document to the TDIA or to a law enforcement agency as soon as the loss is discovered.

Easy means for reporting lost or stolen documents such as a toll-free phone number, fax, online, or in person should be in place and easily accessible to public. Guidance should also be easily accessible to citizens who lose a passport overseas. Such guidance should also highlight that once a travel document is reported lost or stolen, it will be cancelled and no longer valid for travel. A new application to replace the document will be necessary. If subsequently recovered, the document cannot be re-validated, and should be submitted to the issuing authority for physical cancellation or destruction.

When a passport is reported lost or stolen, a written report should be completed by the person reporting the loss or theft and the issuing authority should ensure that sufficient personal questions are asked to be able to determine if the reporter is the genuine holder.

In some countries it is an offence to fail to report the loss or theft of a passport as soon as the loss is discovered. It may also be an offence to use a cancelled passport to travel, even by a genuine holder.

Examples of public awareness tools on reporting lost and stolen travel documents

- US: http://travel.state.gov/passport/lost/us/us_848.html
- Canada: http://www.ppt.gc.ca/planification/203.aspx?lang=eng
- Australia: https://www.passports.gov.au/Web/LostStolenInfo.aspx
- New Zealand: http://www.passports.govt.nz/diawebsite.nsf/wpg_URL/Services-Passports-Lost-or-Stolen-Passports

10.2.2 Stricter Policies for Reapplication

Stricter policies for applicants with a lost or stolen travel document history will provide incentive for holders to take good care of their document. Recommended policy deterrents for consideration include, but are not limited to:

- Applicant should be treated as first time travel document applicants (where countries also have a simplified renewal process).
- the requirement to appear in person for the replacement application;
- a personal interview;
- higher fees for the replacement;
- mandatory endorsement identifying the document as a replacement—this will tend to draw the attention of border control and immigration officers;
- mandatory hold time between application and issuance to permit investigation;
- limitation of the validity of replacement travel documents; and
- (if applicable by law) a refusal to issue another travel document after, for example, a second lost document or where there is evidence that a reported stolen document was actually sold or loaned.

Applications to issue a replacement for a lost or stolen passport or other travel document represent a potential vulnerability and should be screened and investigated for fraud by adjudication/entitlement staff. In the case of multiple losses, a personal interview with the applicant and a police investigation might be required. Several elements can lead a person to falsely declare a travel document lost or stolen to get a replacement one:

- border crossing or customs restrictions have been entered in the existing document;
- the applicant is attempting to maintain temporary residence against the regulations of a country by obtaining a new passport which shows no previous entry stamps;
- the applicant is trying to circumvent another country's immigration or other laws; or
- the travel document contains suspicious visa pages.

10.3 Mitigation Measures

Mitigation measures to reduce the security risks posed by lost and stolen documents include the immediate cancellation of reported lost and stolen documents, reporting them to a national database, and sharing this information with national and international partners.

10.3.1 Cancellation of Lost or Stolen Travel Documents

Once a passport or another travel document is reported lost or stolen, it should immediately be cancelled and declared invalid for travel. This is applicable to both personalized (regular, diplomatic, official, special, temporary/emergency passports) and blank documents. A new application by the holder to replace the document will be necessary.

In many cases, a document reported lost or stolen is subsequently found by the rightful holder. In such cases, the document should remain invalid, not be returned to circulation, and be submitted to the TDIA for physical cancellation or destruction. Use of travel documents reported lost or stolen by the genuine holder may cause the traveller considerable inconvenience and added expense. The traveller may not be permitted to board an aircraft or may be refused entry or detained at his or her destination.

10.3.2 Reporting to a National Lost or Stolen Travel Document Database

A lost or stolen travel document should be declared invalid and be immediately listed on a lost or stolen travel document database for at least as long as the validity period of the document. It is recommended that each government maintain a database that can be accessed as part of the border crossing process. The lost or stolen data should be uploaded regularly, preferably on a daily basis. Special care should be given to the accuracy and integrity of data to avoid inconvenience to compliant travellers at the border having not reported a lost or stolen document. If an error is confirmed, the issuing authority should take all necessary measures to remove the relevant document data from the database.

The use of serial numbers for each blank and personalized travel document facilitates the cancellation of the document if it is reported lost or stolen. Reusing travel document or book numbers throughout the lifetime of an individual makes it more difficult to track a lost or stolen document and increases the likelihood that the holder will have problems at the border.

Exchange of information on lost or stolen travel documents is a key risk mitigation strategy in relation to border control, immigration and identity theft. As such it is important for border and immigration officers at all ports of entry to screen all national passports (and other travel documents) presented against the database to verify whether they have been reported lost or stolen. This information should be accessible in real time. The lost and stolen database should be equally available to law enforcement authorities, to detect cases of identity theft, and to visa issuing authorities to prevent visas being issued in lost or stolen documents.

National lost and stolen travel document databases can provide information which can be analyzed and used to assess threats related to national travel documents and the issuance process. In order to use the database for this purpose it should include detailed information about individual and collective losses of travel documents.

10.3.3 International Information Sharing

Through their national database, countries are now commonly able to identify the use of their own lost and stolen travel documents when presented at their national border. However, in order to determine whether a foreign travel document presented at the border has been declared lost or stolen countries much share information on lost and stolen travel documents with international partners. In addition to potential bilateral or regional data exchange, international partnerships exist to facilitate the exchange of lost and stolen travel document data. Examples are the Interpol Stolen and Lost Travel Documents (SLTD) Database and the APEC Regional Movement Alert System (RMAS).

Global interchange of information on lost and stolen travel documents provides improved border integrity and helps identify identity theft either at the border or in other situations where travel documents are presented as a form of identification.

10.3.3..1 Interpol Stolen and Lost Travel Documents (SLTD) database

Interpol manages a database known as the Stolen and Lost Travel Documents (SLTD) database which contains detailed information on passports, identity cards, visas etc. reported lost or stolen by

countries all over the world. It enables front-line border control and immigration officers to instantly check whether a travel document presented by a traveller has been reported stolen or lost.

All TDIAs should report details pertaining to lost and stolen travel documents to Interpol as soon as possible, preferably within 24 hours of receiving the data. This includes blank passport books and personalized documents. National databases can assist with the transfer of the required information to the Interpol SLTD.

A central office or clearly designated authorities from each country should be responsible for reporting this data to Interpol to ensure that law enforcement authorities know where to report lost or stolen data and to ensure that the data is regularly transmitted to Interpol. Countries should ensure that their Interpol National Central Bureau (NCB) is aware of the procedures for reporting, updating and verifying its lost or stolen travel document information to Interpol.

The information to be submitted to Interpol SLTD should include, but may not be limited to:

a) document number as displayed in the MRZ (or serial number in a blank book)
b) type of document, i.e. passport or other
c) issuing country's ICAO Code
d) whether the document was issued or blank
e) whether the document was lost or stolen
f) date and place of issuance
g) date and place of theft or loss.

Care should be taken to ensure the quality, completeness and accuracy of data, more particularly of the document number. Any input error can have consequences for genuine travellers and can be costly for the issuing authority, e.g. if the traveller seeks compensation and the issuing authority is at fault. If an error is confirmed, the issuing authority should take all necessary procedures to remove the relevant document data from the database.

Each country should endeavour to make the Interpol SLTD available to front-line border control and immigration officials for real time screening of all arriving at ports of entry. The database should be available to visa issuing authorities in order to prevent visas from being issued into lost or stolen documents and to law enforcement authorities to detect identity theft. It is recommended that TDIAs make available to Interpol a 24/7 contact to confirm the status of reported documents and to resolve Hits in the Interpol database on a timely manner.

To help countries connect easily, Interpol has developed two integrated solutions using either fixed or mobile integrated network databases, known as FIND and MIND. Both can integrate into the existing computer-assisted verification system of a country. In addition, MIND can also be used in a country without an existing system. Access to international data and integration into existing systems are the two main benefits of using MIND or FIND.

⇒ Interpol website on MIND and FIND: www.interpol.int/Public/FindAndMind/Default.asp

The Interpol SLTD initiative is widely endorsed by several international fora including ICAO, G8, EU, OSCE (Decision no 4/04 reporting lost/stolen passports to Interpol's automated search facility/stolen travel document database) and the United Nations (Security Council Resolution 1617).

⇒ Guidance documents developed by the G8 Roma-Lyon Migration Expert Sub-Group:
  - Processing Travellers who Present Lost and Stolen Travel Documents
  - G8 Best Practices on Quality Control of Reporting on Lost and Stolen Travel Document Data

⇒ OSCE Decision no 4/04: www.osce.org/documents/mcs/2004/12/3907_en.pdf
⇒ UN Security Council Resolution 1617: http://daccessdds.un.org/doc/UNDOC/GEN/N05/446/60/PDF/N0544660.pdf?OpenElement

The Regional Movement Alert System (RMAS) is an APEC initiative enabling positive validation of passports. RMAS enables participating economies to verify the status of passports in real time at the source, and alert the relevant agencies if action is required. In addition to checking for lost, stolen and invalid passports, RMAS is able to determine whether a passport is recognized by its issuing authority as having been validly issued.

⇒ APEC RMAS: http://www.businessmobility.org/RMAL/RMAL.html

11 Overseas Issuance

11.1 Summary

Travel documents issued abroad are usually issued in much smaller quantities than domestically issued travel documents, and are often under the jurisdiction of a different department of government than those issued domestically. Despite this fact, it is important that the security of the issuance process be equivalent to the domestic one, including all the best practices exposed in the various chapters of this guide. Headquarters should oversee the work processed at the mission to ensure that these security best practices are followed at all times.

To ensure uniformity and security of the entitlement process and the personalization of travel documents, some countries repatriate one or both of these functions to their headquarters. Of course this lengthens the time required for the issuance and delivery of travel documents and may have an impact on the number of temporary and emergency travel documents issued. This chapter discusses the cases where the entitlement and personalization functions are done in missions abroad.

11.2 Overseeing of Work

Locally engaged staff sometimes carry out issuance functions at missions. It is therefore important that they be thoroughly security screened to the same level as passport personnel in the home country. Their activities in the issuance process should be monitored to the same level as domestic employees. Overseas staff should receive the same training as personnel in the home country, including security briefing, training and awareness. The policies, entitlement criteria, documentary evidence of citizenship and identity, application requirements, etc. should also be virtually identical to those in the home country.

There should be constant communication between headquarters and missions to ensure issuance policies and practices are known and well understood by missions. Audits, reviews, spot checks and quality control should be performed on a regular basis by headquarters to ensure that all policies and practices are being enforced in all missions overseas. Good communications between the country and missions, as well as good working conditions, help create a sense of ownership for locally engaged staff, which encourages loyalty to the country.

11.3 Entitlement

When entitlement is done by locally engaged staff, a supervisor who is citizen of the country should always approve the work done on the application including review of the applicant documentary evidence, social footprint, guarantor checks and reference checks. Consular staff should provide the final authorization of any travel document entitlement decision.

Missions abroad issuing travel documents should, wherever possible, have online access to the same databases, clearances, watch lists and travel restriction data as domestic offices. When in doubt about the integrity of the information and/or documents provided by the applicant or about how to interpret entitlement policies, the case should be referred to headquarters. Travel documents issued by missions should be included in any national databases.

11.4 Personalization

The books personalized overseas should use the same personalization (printing) technology and stock, including security features, as the books produced in the home country.

Control of blank books needs to be even tighter abroad than at domestic facilities. The same best practices described in Chapters 4 and 5 should apply to overseas issuance. Travel document blanks should be kept in the secure area of the mission and only the officers responsible for travel document issuance should have access to the blank books. If locally engaged staff is personalizing travel documents, a senior consulate staff, a citizen of the country, should always supervise the work and perform quality control. As done at headquarters, accounting of blank books should be done by at least two employees, including a citizen of the country, at the beginning and the end of each day.

12 National and International Stakeholders

12.1 Summary

Documents issued by the TDIA are used and verified by several national and international stakeholders. Reciprocally, to ensure the security of its documents and issuing process, the TDIA must consult and be in contact with several national, international and private partners. This section lists the major partners and stakeholders the issuing authority should be in contact with, and the kind of information and data that should be bilaterally communicated.

12.2 National Stakeholders

The TDIA should have active partnerships with national authorities that are stakeholders in the issuance and use of travel documents. These organizations should include, but not be limited to:

- Border Control
- Immigration
- Law Enforcement or Police
- Forensic document laboratory
- Other organizations involved in developing and feeding watch lists and travel restrictions for the purpose of travel document entitlement
- Vital Statistics, i.e. breeders/primary and supporting documentation issuers
- Any other partners involved in the travel document issuance process, e.g. overseas issuance; diplomatic, special, official passport issuance; organizations accepting applications.

All these organizations may either contribute to the development of the physical characteristics of the travel document; influence entitlement decisions; have an impact on the security of the issuance process; or may be affected by any changes or decisions made by the TDIA related to the travel document and its issuance process.

12.2.1 Border Control and Immigration

Border control and immigration authorities are the TDIAs closest partners. They determine who can enter the national territory and who cannot, based in large part on an examination of the travel document that a traveller carries. Border and immigration officers know which security features are the most effective and more easily verified at both primary and secondary inspections.

As first line users, border control and immigration authorities also witness and collect data on incidences and trends in travel document fraud. TDIAs should communicate regularly with these authorities and develop partnership to exchange information on fraud and inform the development, design and integration of security features into travel documents. The TDIA should take all appropriate steps to ensure that any technical or physical features they introduce into travel documents are developed in consultation with and in consideration of border control and immigration requirements.

When new security features, new versions or specifications are introduced into a passport, border and immigration officers both nationally and internationally should be advised within a reasonable timeframe. Cooperation and communication with border control and immigration authorities is also essential to ensure that the introduction of new versions or upgrades to travel documents, such as the national introduction of ePassports, be interoperable with existing and future border control systems and infrastructures, e.g. readers, automated border control, software.

Border control and immigration authorities may contribute to watch lists used in the travel document entitlement process. The TDIA reciprocally shares data on reported lost, stolen or cancelled passports with border and immigration authorities. There should also be bilateral communication mechanisms in place to confirm the validity of the data provided by both organizations.

12.2.2 Law Enforcement, Police, and Forensic Document Laboratory

Law enforcement, police and forensic document laboratories are also well aware of security threats to travel documents and trends in fraud. They investigate cases of travel document fraud and counterfeit techniques. This information is invaluable to the TDIA for the development, design and integration of security features into travel documents as well as for the integration of security mechanisms and internal controls in the issuance process.

Law enforcement and police also feed data to watch lists and travel restriction lists which are used during the travel document entitlement process.

12.2.3 Vital Statistics

The entitlement decision requires the verification of identity and citizenship using breeder/primary and supporting documentation often issued by separate governmental organizations. There should be frequent communications with these organizations to obtain information on the different document versions being issued, the security features they include and fraud related information. There should also be a mechanism in place to regularly verify the integrity of the documents submitted by applicants. As stated in Chapter 4, direct electronic access to appropriate records or registers is recommended.

12.2.4 Others

Authorities providing data to watch lists and travel restrictions

The data included in the various watch lists and travel restrictions lists used for entitlement decisions vary in each state. Border control, immigration and law enforcement authorities should contribute data to these lists. Additionally, Justice Authorities, Correctional Services, Foreign Affairs authorities, Tax Collection Services, etc. may also contribute.

Partners involved in the issuance process

All organizations involved in the issuance process, including overseas issuance; diplomatic, special, official passport issuance; and organizations that accept applications on behalf of the TDIA, should be involved in, and made aware of any policy/process changes introduced by the TDIA that may have an impact on the security of the issuance process.

12.3 International Partners

The TDIA should have active associations or partnerships with other nations, and participate in international fora and working groups, to share information on travel document standards, specifications, trends and frauds; share relevant travel document data; and, seek capacity building help if required. These organizations should/could include, but not be limited to:

- International Civil Aviation Organization (ICAO)
- Interpol
- Asia-Pacific Economic Partnership (APEC)
- International Organization for Migration (IOM)
- Organization for Security and Cooperation in Europe (OSCE)
- Organization of American States (OAS)
- Any other regional and/or international fora focusing on travel document, border security, migration, etc.

12.3.1 International Civil Aviation Organization (ICAO)

ICAO establishes the standards and recommended practices on passports and other travel documents (Section 3 of Annex 9 of the Chicago Convention). The ICAO Technical Advisory Group on Machine Readable Travel Document (TAG/MRTD) develops and adopts specifications for travel documents which are included in Document 9303. The TAG/MRTD also publishes guidance material as well as Technical Reports and Information Papers to assist States in implementing its specifications. Under the governance of the TAG/MRTD, two working groups were established:

The New Technologies Working Group (NTWG)
In partnership with the International Organization for Standardization (ISO), the NTWG develops strategies, policies and guidance material related to the manufacture, security, testing, issuance, deployment and globally interoperable use of MRTDs and eMRTDs in both physical and electronic form.

The Implementation and Capacity Building Working Group (ICBWG)
ICBWG Supports the ICAO Secretariat in carrying out capacity building outreach activities to help ICAO Member States issuing MRTDs and improving security of their issuance process.

The ICAO Secretariat—MRTD Program should be contacted for any need of funds or expertise related to the issuance of identity and travel documents.

⇒ MRTD Program: http://www2.icao.int/en/MRTD/Pages/default.aspx
⇒ To order Document 9303: http://www2.icao.int/en/MRTD/Pages/OrderICAOPublication.aspx

12.3.2 International Data and Information Sharing

As mentioned in Chapter 10, it is recommended that information on travel documents reported lost or stolen be shared with international partners. Sharing this information enables countries to identify the use or level of abuse of their own lost and stolen passport but also that of the documents issued by other countries. The Interpol Stolen and Lost Travel Documents (SLTD) database enables front-line officers to check instantly whether a travel document is stolen or lost. In addition to checking for lost, stolen and invalid passports, the Asia-Pacific Economic Cooperation (APEC) Regional Movement Alert System (RMAS) is able to determine whether a passport is recognized by its issuing authority as having been validly issued.

Several Bilateral, regional and international partnerships have been established worldwide to facilitate and improve cooperation and sharing of data between allies and to facilitate border crossing between neighbour states. Examples include the Shengen Area, MERCOSUR, ECOWAS, CARICOM, etc.

12.3.3 International cooperation and capacity building

In addition to ICAO, there are several international and regional entities with capacity programs, expertise, funding and/or resources available to help and collaborate with countries needing some help in the field of issuance of travel documents. IOM, OAS and OSCE are some examples of active organizations in this domain.

International Organization for Migration (IOM)—Technical Cooperation on Migration Management and Capacity Building
IOM is an intergovernmental organization of 122 members. The activities of IOM's Technical Cooperation on Migration (TCM) division help governments equip themselves with the necessary policy, legislation, administrative structures, operational systems and human resource base needed to tackle diverse migration problems. IOM offers advisory services, technical assistance and training activities.

⇒ IOM TCM: http://www.iom.int/jahia/Jahia/pid/749

Organization of American States (OAS) — Inter-American Committee Against Terrorism (CICTE)
The main purpose of the Inter-American Committee Against Terrorism (CICTE) is to promote and develop cooperation among member states to prevent, combat, and eliminate terrorism. The Document Security and Fraud Prevention program has for objective to improve the ability of target countries' law enforcement, customs and immigrations personnel to improve their controls on the issuance of travel and identity documents and their capability to detect fraudulent documents, in order to prevent their counterfeiting, forgery, or fraudulent use.

⇒ OAS CICTE: http://www.cicte.oas.org/Rev/En/

Organization for Security and Cooperation in Europe (OSCE) — Action Against Terrorism Unit (ATU)
Established in 2002, the OSCE Action Against Terrorism Unit is the Organization's focal point for coordinating and facilitating OSCE initiatives and capacity-building programmes in combating terrorism. The Travel Document Security Programme delivers practical assistance and guidance in the implementation of anti-terrorism commitments. The OSCE has led numerous capacity building activities in the past years, including workshops on Travel Document Security and Handling and Issuance of Travel Documents as well as Forged Document Training.

⇒ OSCE ATU: http://www.osce.org/atu/

12.4 Private Partners

In addition to national and international partners, there are benefits for both the TDIA and private companies to remain in contact and exchange information.

12.4.1 Airlines

As governments are demanding more and more from the airlines, from verifying travel document integrity to storing and communicating passenger information, it is a good idea for the TDIA to remain in contact with airlines and associations, e.g. IATA to share information on travel document characteristics and security features.

12.4.2 Private companies

The International Organization for Standardization (ISO) and private companies evolving in the field of travel documents, readers, chips, biometrics, printers, etc. are excellent sources of information on new available technologies, systems, and processes. To undertake regular Requests for Information (RFI) is a good practice to remain aware of latest research and innovations.

Reference Documentation

1. *Security Standards for Machine Readable Travel Documents* — Informative Annex of Document 9303
2. *Minimum Security Standards for the handling of MRTDs and other passports* — Informative Annex to Section III of Document 9303
3. *ICAO-New Technologies Working Group (IEC JTC1 SC17 WG3/TF1), "Machine Readable Travel Documents (MRTDs): History, Interoperability, and Implementation"*, Draft 1.4, 7 March 2007, TAG-MRTD/17-WP/16
4. *Recommended Standards for Secure Proof of Status and Nationality Documents to Facilitate Cross-Border Travel, Security and Prosperity Partnership Deliverable* 1.1.3
5. *A Guide to Biometric Technology in Machine Readable Travel Documents*, APEC Business Mobility Group
6. *G8 Best practice for the processing of travellers who present lost of stolen travel documents*
7. *G8 Best practices on quality control of reporting on lost and stolen travel document data*

Abbreviations

ABC	Automated Border Control system
APEC	Asia-Pacific Economic Cooperation
BAC	Basic Access Control
DS	Document Signer
EAC	Extended Access Control
EU	European Union
FIND	Fixed Interpol Network Database
ICAO	International Civil Aviation Organization
ICBWG	Implementation and Capacity Building Working Group
IOM	International Organization for Migration
ISO	International Organization for Standardization
MIND	Mobile Interpol Network Database
MRTD	Machine Readable Travel Document
eMRTD	Electronic Machine Readable Travel Document
MRP	Machine Readable Passport
MRZ	Machine Readable Zone
NCB	Interpol National Central Bureau
NTWG	New Technology Working Group
OAS	Organization for American States
OSCE	Organization for Security and Co-operation in Europe
PKD	Public Key Directory
PKI	Public Key Infrastructure
RFI	Request for Information
RMAS	Regional Movement Alert System
SLTD	Stolen Travel Document Database
TAG	Technical Advisory Group
TDIA	Travel Document Issuing Agency