For Publication on the ICAO Website

Guide for Assessing Security of Handling and Issuance of Travel Documents

2016

File: Guide for Assessing Security of Handling and Issuance of Travel Documents
Author: Subgroup of the Implementation and Capacity Building Working Group (ICBWG), Working group of the ICAO Technical Advisory Group on the Traveller Identification Programme (TAG/TRIP)

General Table of Contents

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 the Seventeenth Meeting of the Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD/17), 20 to 22 March 2007, 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. (TAG/MRTD was renamed TAG/TRIP in 2015 to reflect the role of the group in supporting all elements of the new ICAO Traveller Identification Programme (TRIP) Strategy.)

This guide is divided in three parts:

1) The first part recommends best practices to prevent and mitigate security threats at every step of the travel document issuance process.
2) The second part provides a comprehensive evaluation tool checklist to assess the issuance process vulnerabilities.
3) The third part is a guide for experts which contains a series of templates containing a summary of what's important in each chapter of the Guide.

The measures and practices presented in this document are recommended practices and as such no country is required to adopt them. However, if implemented they can provide a strong defense against fraud.

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
4	January 2016	Update and describe links; add section on civil registries in Chapter 3; provide search terms for web resources rather than links; add clarity to IT Security sections; add Part 3; include reference to TRIP; add description of PKI; update references to Doc 9303 and Annex 9 – Facilitation; include comments from ICBWG. Approved by TAG/TRIP/1 (30 March to 1 April, 2016) for publication. Published on the ICAO public website, March 2017.

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 or immigration status 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 travel document enables the holder to apply for a visa for those countries that require it upon entry, and allows the authority to annotate the travel document, and record entry and exit dates.

In addition to travel purposes, travel documents 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 travel document can be used for espionage, financial crimes, and 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 travel documents 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 may be used to establish identity as part of the travel document application process. 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 travel 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 altered, 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 travel document 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 passport, and other travel documents, is a key component of national and international anti-crime and anti-terrorism strategies. 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.

While travel document 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 at 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. Chapter 3 of Annex 9 - *Facilitation* to the Convention on International Civil Aviation 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 (re-named TAG/TRIP in 2015) develops and adopts specifications for MRTDs and eMRTDs, which are included in Document 9303. TAG/TRIP 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/TRIP, two working groups operate: 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. At the Nineteenth Meeting of TAG/MRTD in December 2009 the Guide was approved for publication.

Amendment 24 to Annex 9 - *Facilitation* included a Standard requiring States to establish appropriate controls over the entire travel document application, adjudication and issuance processes to ensure a high level of integrity and security (Standard 3.8.1). This Guide can be used to assist States in meeting that Standard.

Internet Resources:

⇒ The Security and Facilitation pages on the ICAO public website (http://www.icao.int/Security/Pages/default.aspx) include information on the TRIP Strategy and MRTD Programme. They provide information on travel document specifications, guidance material and Technical Reports, meeting reports, the ICAO TRIP Magazine etc. (Use search terms: ICAO MRTD Programme.)

⇒ ICAO Document 9303, providing the specifications for Machine Readable Travel Documents, can be downloaded for free from the ICAO website. (Use search terms: ICAO Document 9303.)

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 travel document 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, travel document 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 travel document issuance remain essential, but are performed prior to an application for a travel document, in a separate civil registration process. The content of this guide therefore remains relevant to all travel document issuance systems, albeit the sections on enrolment and identity verification may need to be read as applying to civil registration as well as travel document 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 an informative annex to Document 9303. This valuable paper, 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 travel document 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. Should countries devise alternative methods of achieving the same aims that reflect their own circumstances, the ICBWG invites them to inform the group so that consideration can be given to sharing these as recommendations for best practice in future editions.

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

- application intake;
- the decision-making and business processes to establish an individual's identity, citizenship or immigration status and travel restrictions;
- production;
- personalization; 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 travel document 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 travel document 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.

Part 3 — A Guide for Experts contains a series of templates containing a summary of what's important in each chapter of the Guide. It is designed for use by experts.

For Publication on the ICAO Website

Guide for Assessing Security of Handling and Issuance of Travel Documents

Part 1- Best Practices on Secure Issuance of Travel Documents

Version: Release 4

February 2016

File: Guide for Assessing Security of Handling and Issuance of Travel Documents

Author: Subgroup of the Implementation and Capacity Building Working Group (ICBWG), Working group of the ICAO Technical Advisory Group on the Traveller Identification Programme (TAG/TRIP)

Table of Contents for Part 1
Best Practices on Secure Issuance of Travel Documents

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

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 The TDIA should be an independent governmental organization (or section) focussing only on the issuance of passports, travel documents and other government documents. An independent organization would not be unduly influenced or subject to decision making by senior officials who may have other priorities or conflicting interests

A single issuing authority would:

- ensure an organization's ability to develop expertise in travel document issuance;
- ensure continuity and consistent practises across the issuance process;
- ensure a fair process where all applicants are treated fairly and in accordance with the law to mitigate the risk of corruption; and
- be more secure and more cost effective than separate authorities for each document type.

Where travel documents are issued by more than one Government Department, it is essential that consistency is achieved with regard to security of the processes. There must be coordination on the following elements:

- The document signing system used to add digital security to ePassports must be common across the Departments involved, in part because ICAO recognizes only one Public Key Directory member per country.
- A consolidated register of issued and revoked passports should be maintained which is accessible to immigration agencies and other government entities having a legitimate reason to access the information.
- A consolidated reporting should be made to Interpol so that information on lost and stolen passports can be added in a timely manner to the Interpol SLTD database (see 10.3.3..1).

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. The responsibilities of authorities at the national, regional and local levels should all be clearly defined. 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;
- mechanisms to prosecute forgery, improper use of travel documents, false representation – use of someone else's travel document, and mutilation of the travel document;
- access to information; and
- clear statements of the behaviour expected of staff members and other associated workers of the TDIA to ensure the highest levels of integrity, along with penalties for failing to uphold these standards.

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 travel document 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 and/or fees;
- personalization; 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 its own conclusion based on its 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 capable of detecting and deterring threats both internal and external.

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. Attendance at ICAO MRTD/TRIP Symposia and Regional Seminars (and other ICAO meetings) and security document industry events may also provide valuable information on current and future technologies and systems. 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 partners' facilities and processes 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 so that each can become experts in their respective functions and decisions on files would be impartial. Independence would also ensure a more objective review of the security aspects of files – both in cases of travel document misuse/abuse and in the event of internal malfeasance. There would be no conflicts of mandate and priorities during peak processing times for example. Separation of responsibility would better enable security to conduct internal audits, review and analysis or investigation for malfeasance if necessary.

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.

Where the TDIA is small and does not have the resources to meet this recommendation of having a security team, this function should be assigned to one of the senior staff who should be trained on what to look for and be able to influence how staff is trained on security. This person should also carry out simple security sweeps/audits.

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 and/or 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.

Where the TDIA is small this recommendation could be fulfilled by the senior person responsible for security noted in section 1.3.1.

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 travel document 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.

As above, where the TDIA is small, this function may also need to be covered by a senior manager responsible for security.

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 and used at the basic level to enforce proper application of practices and procedures by staff. They need to be kept up to date and relevant. Written documentation will allow for consistency through staff turnovers, allow for easier training of both operations and security, and allow for management reviews and to set the rules.

Written documentation 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 organizations involved with travel document issuance. This will ensure compliance; fair and equitable treatment of all applicants in accordance with principles of natural justice and procedural fairness, mitigate the risk of corruption, and facilitate investigations relating to internal malfeasance.

The policies, practices and guidelines should outline the responsibilities of all individuals with regard to security 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.

1.3.3..2Financial 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 organized crime or 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 consequences 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.

To ensure sufficient funds for security, 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, information technology security, brochures, communication materials, audits and reviews by external parties.

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. Where this is not possible, it is essential that workload levels are monitored closely and that plans are in place to deal with unusual patterns of demand.

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. This is the sort of environment where fraud may be more easily perpetrated as staff have less time to ask the extra question or are simply too busy. 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.[Suggested Reference (for purchase) Australian and New Zealand Risk Management Standard ISO 31000 (Use search terms: AS/NZS ISO 31000:2009 Risk management - Principles and guidelines].

Error! Hyperlink reference not valid. When considering risks and vulnerabilities the TDIA should also develop a Business Continuity Plan to ensure that, if a major threat or attack materialises, travel document 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. Use search terms: Business Continuity Institute.

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.

1.4.1..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 omit some necessary processes 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.

1.4.1..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, submission of documentary evidence, submission of photographs, and in some cases secondary biometrics. The information and documentation they provide will enable TDIA employees to determine an applicant's identity, their eligibility to apply and their entitlement 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, applications should be processed in a uniform manner throughout the TDIA; these should be documented for audit and public information purposes. Application forms should also be standardized and the requirements the applicant must comply with should be consistent across the country. This will ensure fair and equitable treatment of all applicants; mitigate the risk of corruption; facilitate investigations relating to internal malfeasance and should a case go to court, processes can be justified if they are consistent. 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	There should be rigorous processes available to reliably link an individual with a claimed identity. A first-time application should be scrutinized extremely carefully. Applicants who have had a previous travel document 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 travel document in their application. However, if this previous travel document 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 (whether in paper or electronic formats) or applying at partner's offices (i.e. passport agents) 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) and consideration given to changing the applicant's behaviour, perhaps through only supplying limited validity travel

	documents or through charging increased fees.
Collection of secondary biometrics	Capture of secondary biometrics 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 and online transactions are not possible, 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 of forms, transmission of data, transmission of digital photographs, and 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 or other authorized 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 travel document 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, such as facial recognition technology, using other secure identity documents to support applications, and information sharing between agencies to verify identity can effectively mitigate the security risks to an acceptable level. In cases where personal attendance requirements are relaxed or reduced, it would be good practice to require personal attendance to at least a small proportion of applicants on a random or risk-based basis.

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 travel document 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.

Travel document application acceptance agents (who represent applicants), if they are used at all, should be officially authorised and (ideally) registered. They must be trained and should have detailed written guidance on how to identify travel document applicants, how to note the identifying documents on the travel document application, and what to do in the event that they are not satisfied with the identity documents presented. Background checks should be performed on acceptance agents at initial registration or authorisation and then on regular or random occasions. 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.

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, the Doc 9303 specifications and/or the state's requirements should be made available to commercial photographers as well as the public.

Examples of published photo specifications for different States can be seen on the Internet using the following search terms: Passport Photo Guidelines [Country Name].

Printed versions of photos should be signed by a guarantor or stamped by the photographer to claim the photo is a true likeness of the person.

With the development of new technologies, some countries may start accepting online applications with 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. If the chain of custody (transfer of the photo) is not secure, and to minimize the risk of the photograph being altered at various steps of the application process, a hard-copy photograph, with a guarantor's signature or photographer's stamp should be required in addition to the digitized photograph.

2.4 Secondary Biometrics

Many countries require, or will require collection of a biometric identifier beyond the facial image 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. If additional biometrics are taken, use can be made of them to simplify renewal processes, where applicable.

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, espionage, 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 personal information, usually sensitive and sometimes quite detailed. 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. In this way a TDIA can keep track of all applications received and when they were received. If an applicant calls about the status of the application, the information will be logged. 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 to ensure that staff is not accessing files for the sake of curiosity. 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 unauthorized personnel 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 saved on or shared through an unprotected network, internet connections or unsecured 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 eMRTDs) should be carefully and securely stored for ease of future reference in appropriately locked cabinets or protected rooms and in appropriate security-protected databases. In some climates the TDIA must take into consideration environmental conditions in which paper records may quickly disintegrate. 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.

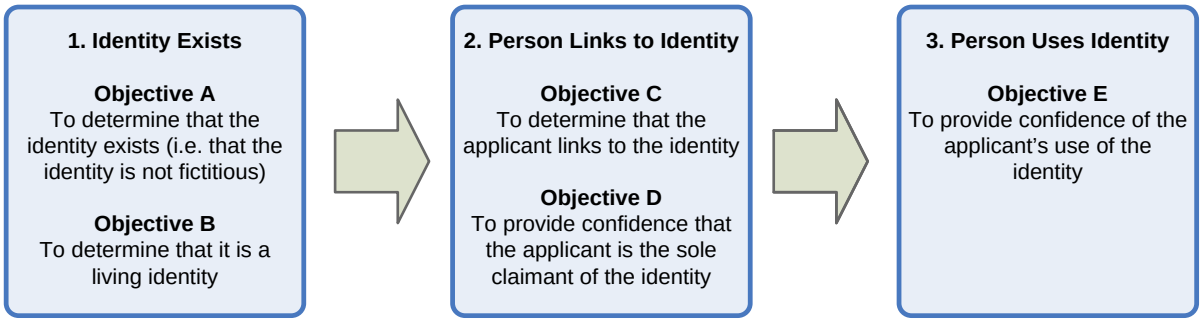
2.5.1 Automated Systems

Using technology to automate travel document issuance processes can increase the security of the issuance process and enhance accuracy if properly designed. 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 accuracy of the data and the rapidity of detection of fraudulent or questionable information. Automated systems should include a random or risk-based 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. This is done through 'evidence of identity' (EOI). EOI refers to the establishment of evidence that, when combined, provides confidence that an individual is who they claim to be (i.e. a driver licence, passport or birth certificate). The diagram below outlines the three key principles (1-3) and five underlying objectives (A-E) that are central to most EOI frameworks or standards, and should be central to the EOI processes a Travel Document Issuing Authority (TDIA) or Border Control Authority (BCA) undertakes as part of its issuance processes:



A robust and secure travel document issuance process should seek to fulfil each of the three principles to a high level of confidence, especially the first time a travel document is issued to that person. If the first interaction is strong, then the TDIA can leverage the strength of the first issuance process for subsequent interactions such as a renewal application, or the replacement of a lost or stolen travel document.

TDIAs should refer to ICAO's Guidance on Evidence of Identification, available on the ICAO MRTD website, for further information on establishing and validating identity for the purposes of issuing a travel document.

To verify identity and citizenship, documentary evidence is usually required by the TDIA. Reference to secure databases of identity, citizenship, and civil registration may be utilised instead of relying upon physical documents. 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 travel document. 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 travel document expired less than one year before the application for renewal.

An example of specific conditions for a simplified renewal process can be found on the Internet using the following search terms: passport simplified renewal process.

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 (see 3.6.4) 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 own identity. TDIAs may also verify the parent's identity or verify against watchlists that there are no known concerns about them e.g. fraudulent applications, previous child abduction charges etc. Children shall not be included in an adult's travel document; rather, each child, including a newborn infant, must be issued with his or her own travel document. (See One-Person One-Passport at 6.4.2)

3.4 Documentary Evidence

Confirmation of the identity of a travel document applicant 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.

In some countries identity and citizenship can be established through reference to secure databases, but documentary evidence to establish entitlement under identity and citizenship requirements is often 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, source, or primary documents. Breeder documents are those that bear identifying details and/or nationality and are issued by a trusted government or other official source. These documents should have been subject to a sufficiently high level of verification by trusted personnel before being issued. Where this is not the case, TDIA should ensure that sufficient steps are taken to provide the level of assurance required to establish identity. This may include additional evidentiary documentation or other means of satisfactorily establishing identity.

The breeder document should contain basic security features including a unique number and potentially a biometric or clear photograph. Without those features, or independent verification through a secure database, 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. In such cases, the applicant could 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

The TDIA should keep in mind the potential that supporting documents may also have been fraudulently issued or issued without sufficient checks.

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 or through secure databases of civil registration or identity.

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 Evidence of Identity Standard is a useful reference and can be found on the Internet using the following search terms: New Zealand Government Evidence of Identity Standard.

In countries where civil registries are in use, these are an effective means to establish whether an identity is real and belonging to a living person and whether this person is a citizen of the state from which he is applying for a travel document.

In some cases a TDIA may be faced with a lack of a proper civil registration system – for example where it was not mandatory to register births or where the system is found to be unreliable. In some cases birth certificates may be issued without much checking of the person's identity. In such situations it is not unusual for other records to be similarly unavailable. Each situation is likely to be different, however, the aim is to improve the ability to establish identity to as high a level as possible. Where the application form contains not only data on the applicant but also on the applicant's parents, it provides an opportunity to check that the applicant can accurately provide information on their names and dates of birth/ages. It may also be possible to identify other family relatives who have also been issued passports and to cross check the applicant's knowledge of them.

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 travel documents are examples of government-owned databases available, for a fee, to all issuing authorities worldwide. A public version of EDISON is available for free on internet at www.edisontd.net.

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. electronic civil registries, 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. TDIAs should consider working closely with civil registry authorities to ensure that civil registry certificates are issued in a secure manner, that lost/stolen certificates are notified to TDIA, that birth certificates are secure documents (i.e. have some security features and are numbered)

3.5 Civil Registries (CR)

Civil registries (CR), where available, are a powerful tool within the issuance process of travel documents. They provide the TDIA with valuable information, help to prevent a travel document being obtained fraudulently and can shorten the time used for verification tasks within the issuance process.

3.5.1 Characteristics

The principal value of civil registration information for the TDIA is that it provides trustworthy certificates and records in respect of travel document applicants. This can be an essential element of the overall travel document application process. It is therefore crucial that both the TDIA and the CR authority work closely together to ensure that these certificates and records can be relied upon. This means that certificates and records must be adequately protected against manipulation or theft. Certificates in particular must be treated in a similar manner to blank travel documents and must be accounted for. Details of any lost/ stolen blank certificates must be passed to the TDIA as they may be presented as part of a travel document application. The TDIA can play an important role in working with the CR authority to advise on the steps necessary to ensure the security of the certificate issuance and in relation to CR records. It should also be noted that where an assessment is carried out of the travel document issuance process, CR is inevitably included. Recommendations from such assessments can have beneficial value for the CR authority, for example, by recommending computerization of records where none exists or the sharing of electronic databases that can be accessed by not only the TDIA but by other Government departments.

3.5.2 Centralized or decentralized

The choice between centralized or decentralized civil registration systems will mostly depend on the country's history, the geography and the political system.

The centralized system offers many advantages, including the standardization of procedures and methods, easier enforcement of improvements in administrative processes and smaller coordination needs. Especially when issuing travel documents a centralized system has the advantage that it can be accessed by all authorized issuing authorities, including national representations abroad (Embassies/Consulates).

The decentralized system may be more suitable for countries with large populations or a strong regional autonomy. Efficient processes for sharing information with the TDIA should be established with each authority.

Whichever system is chosen, there must be an agency at national level to enforce the legal framework, the minimum standards, policy and uniform practices. This national agency will also provide the rules to allowing each person, registered within the system, a unique identifier and it will govern the access rights to the system.

3.5.3 Confidentiality

Many of the data stored in civil registries are sensitive and must therefore remain confidential and benefit from strongly restraint access. The data should also be protected in such a way that only an identified individual can get the paper copies of its record.

Access to the data stored in civil registries must be strongly monitored and each query must be linked to the person who accessed the data. Those provisions should be part of the civil registration law.

3.5.4 Civil registries in the travel document issuance process

Civil registries may appear in the travel document issuance process in different ways:

- A certificate supporting the identity and the nationality of the applicant may be issued by the authority in charge with the civil registration process and joined to the travel document application form. In this case document security and verification possibilities are extremely important and must be considered.

- Where the civil registries have been computerized, the TDIA may get “online” access to the data enabling to check the data written on the travel document application form. This has the advantage, that a travel document will not be issued based on a falsified civil register form, since the data will always be verified (automatically) online and is most up to date (i. e. the death of a person). The security level of civil registry documents (in paper format) can therefore be limited to a certain level.

3.6 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.

3.6.1 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. For remote areas, internet-based video conference facilities, if available, could be used but care should be taken and ideally the applicant should be on official premises of some sort.

3.6.2 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. Persons of significant standing or reputation in the community may also be considered for this role.

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 may also be elders from the applicant's community who provide confirmation of identity in the absence of civil registration records. Should the desired level of assurance not be provided, further confirmatory evidence may be required.

District administrators are another source of guarantors that may offer an acceptable means of supporting a claimed identity.

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.

3.6.3 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.

3.6.4 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.

3.6.5 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 have the strong potential to limit the individual to one specific identity and curtail their 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.

3.6.5..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 identities. This is particularly

relevant where it is relatively easy to obtain supporting documentation (e.g. birth certificates) to present applications in different identities.

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.

3.6.5..2 Other 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.

3.6.6 Database Checks

It is essential that all applicants are 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. A history of an applicant's changes in biographic details may be of use for future reference.

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 travel document 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 travel document.

3.7 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 travel document 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.

3.8 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 must 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 and electronic chips. The protection and secure management of blank travel documents, raw material and the specialist equipment to turn one into the other 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 maintain up to date documented policies and procedures related to the treatment of materials and blank books. All staff should be aware of these. Procedures for the disposal of sensitive waste and of obsolete or otherwise no longer required specialist equipment should be established and the disposal recorded. 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 unique 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. If present, electronic chips should be locked during transit and storage so that they cannot be written to by unauthorised persons. 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 similarly secured 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). The practice of issuing enough books for several days of production is to be avoided. Only the minimum necessary number of blank books, laminates or other materials should be issued to production staff for the employee's shift. 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 travel documents should be counted back in each night, or at the end of work shifts, by two individuals. The blank books must be assigned to individual staff who must assume responsibility for the safe custody of the books whilst in their hands. Appropriate arrangements must be in place to allow for secure storage of books when staff may go on a break or otherwise be absent from their desks. 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. The senior manager of the issuance facility should be required to carry out a physical audit of the blank books held in the vault each month to ensure that all are accounted for and should sign a suitable register to that effect.

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 or materials 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. Where it is decided not to destroy books on a daily basis, the TDIA needs to put in place very robust systems for ensuring that all such books can be accounted for at any time. In all cases there is no reason for spoiled/damaged books not to be destroyed within one month.

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, or a simple locked door, 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. Alternatively, an applicant can be contacted by telephone, email or SMS to addresses supplied by them to alert them that their document is ready for collection.

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 travel document 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 should monitor the number of unclaimed passports. If, after a period of time, documents are unclaimed the applicant should be contacted. The TDIA should inform applicants that in the event that a travel document is not collected within a specified time, the document will be destroyed and that a new application (and fee) will be necessary. A period of 3 to 6 months may be appropriate before destruction takes place. This timeline for destruction should be published. It is important that unclaimed travel documents are not allowed to build up for long periods and must be securely held. They should be accounted for regularly to ensure that none are missing. Cases of unclaimed travel documents should be investigated for fraud, or at the very least the biographic and biometric details should be flagged on TDIA databases should they reappear in another application.

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. Couriers employed by the UK take a digital photograph of the premises the document has been delivered to and this is stored against the applicant's record .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. (Refer to Chapter 10). The document should be immediately declared invalid and swiftly put into a lost/stolen travel documents 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 travel document 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. More detailed information on document security is available in Doc 9303.

6.2 Machine Readable Travel Documents (MRTDs)

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**.

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 an ICAO Annex 9 – *Facilitation* Standard requiring all ICAO Member States to issue only Machine Readable Passports (MRPs) in accordance with the specifications of Doc 9303.

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 standard. It is recommended that countries that need help to implement their Machine Readable Travel documents program contact the ICAO Secretariat MRTD Program.

6.3 Electronic Machine Readable Travel Documents (eMRTDs)

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 travel

document holder. The data encoded in the chip is protected by Public Key Infrastructure (PKI) cryptographic technology. The ICAO eMRTD specifications are included in **ICAO Doc 9303.** 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) and Password Authenticated Connection Establishment (PACE) are recommended security mechanisms to protect data against unauthorized access. Extended Access Control (EAC) can be used to secure secondary biometrics.

Public Key Infrastructure

The eMRTD Public Key Infrastructure (PKI) is a simplified version of the more generic multi-application PKI. The eMRTD PKI application operates in a completely peer-based user environment, with each State independent and autonomous in the matter of MRTDs and security.

In the eMRTD PKI, each issuing State/Authority establishes a single Certification Authority (CA) that issues all certificates directly to end-entities, including Document Signers. These CAs are referred to as Country Signing Certification Authorities (CSCAs). There are no other CAs in the infrastructure. Receiving States establish trust directly in the keys/certificates of each issuing State or organization's CSCA.

The recorded details in the contactless integrated circuit (IC) of the eMRTD are organized in a standardized Logical Data Structure (LDS) which is defined in Doc 9303. A series of mandatory and optional Data Elements has been defined for the LDS and each of these Data Elements is grouped into logical Data Groups (DGs). For example, DG1 contains the details recorded in the Machine Readable Zone (MRZ) of the passport data page, DG2 contains the photograph of the document holder and so on.

Apart from the LDS, the IC contains a Document Security Object (SOD). The SOD is digitally signed using a Document Signer Certificate (DSC) and is used for checking the authenticity and integrity of the details recorded in the LDS.

The eMRTD Public Key Infrastructure (PKI) enables the creation and subsequent verification of digital signatures on eMRTD objects, including the Document Security Object (SOD) to ensure the signed data is authentic and has not been modified. Revocation of a certificate, failure of the certification path validation procedure or failure of digital signature verification does not on its own cause an eMRTD to be considered invalid. Such a failure means that the electronic verification of the integrity and authenticity of the LDS data has failed and other non-electronic mechanisms could then be used to make that determination as part of the overall inspection of the eMRTD.

Since the CSCA is the root of trust for eMRTDs, it is imperative that the Country Signing CA key pairs are generated and stored in a highly protected offline CA infrastructure by the issuing State. The state should also have control over the issuance of the Document Signers from the CA infrastructure and on the creation of the SOD. This means that the process of personalization of the chip data has to be in the control of the issuing State.

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.

Annex 9 – *Facilitation* of the Chicago Convention (Recommended Practice 3.9) recommends Contracting States incorporate biometric data in their machine readable travel documents as specified in Doc 9303. It should be noted however that this is a recommendation and not a requirement.

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 eMRTD 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 of 2009, the ICAO Council adopted a Recommended Practice related to the ICAO PKD. (See section 6.4.1 on ICAO Standards and Recommended Practices.)

More information on the PKD and how to become a member is available on the Security and Facilitation pages on the ICAO public website (http://www.icao.int/Security/Pages/default.aspx). (Use search terms ICAO MRTD Programme and follow the links under ICAO Public Key Directory (PKD).)

6.4 ICAO Standards, Recommended Practices and Specifications

6.4.1 ICAO Standards and Recommended Practices

Some Standards and Recommended Practices included in Chapter 3 of Annex 9 - *Facilitation* deal specifically with travel document security. TDIAs must comply with these Standards and follow, to the extent possible, the Recommended Practices. (Annex 9 is amended on a regular basis and the most recent version should be referred to in order to ensure up-to-date information. At the time of publication of this Guide, the following Standards and Recommended Practices were in effect (Annex 9 – *Facilitation*, Fourteenth Edition, October 2015):

Document Security
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.

Standard 3.8 - Contracting States shall establish controls to safeguard against the theft of their blank travel documents and the misappropriation of newly issued travel documents.

Standard 3.8.1 - Contracting States shall establish appropriate controls over the entire travel document application, adjudication and issuance processes to ensure a high level of integrity and security.

Travel Document Validity Period
Standard 3.4 — Contracting States shall not extend the validity of their machine-readable travel documents.

Recommended Practice 3.18 – When issuing passports for tourism or business travel, Contracting States should normally provide that such passports be valid for a period of at least five years, for an unlimited number of journeys and for travel to all States and territories. 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 travel document validity period.

One passport/One person
Standard 3.17 - 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 Travel Documents
Standard 3.11 - All passports issued by Contracting States shall be machine readable in accordance with the specifications of Doc 9303, Part 4.

Note. - This provision does not intend to preclude the issuance of non-machine readable passports or temporary travel documents of limited validity in cases of emergency.

Standard 3.11.1 - 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, Machine Readable Travel Documents. The required data stored on the integrated circuit chip is the same as that printed on the data page, that is, the data contained in the machine-readable zone plus the digitized photographic image. Fingerprint image(s) and/or iris image(s) are optional biometrics for Contracting States wishing to supplement the facial image with another biometric in the passport. Contracting States incorporating biometric data in their Machine Readable Passports are to store the data in a contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by ICAO.

ICAO Public Key Directory
Recommended Practice 3.9.1 - Contracting States issuing or intending to issue eMRTDs should join the ICAO Public Key Directory (PKD) and upload their information to the PKD.

Recommended Practice 3.9.2 - Contracting States implementing checks on eMRTDs at border controls should join the ICAO Public Key Directory (PKD) and use the information available from the PKD to validate eMRTDs at border controls.

INTERPOL
Standard 3.10 - Contracting States shall promptly report accurate information about stolen, lost, and revoked travel documents, issued by their State, to INTERPOL for inclusion in the Stolen and Lost Travel Documents (SLTD) database.

Recommended Practice 3.10.1 - Each Contracting State should, as far as practicable, query, at entry and departure border control points, the travel documents of individuals travelling internationally against the INTERPOL Stolen and Lost Travel Documents (SLTD) database.

6.4.2 Document 9303 Specifications

To ensure global interoperability and therefore to enhance security, travel documents must be compliant with the specifications of Document 9303. Machine readable travel documents are required whereas electronically enabled MRTDs (eMRTDs) are recommended but not required. Document 9303 contains specifications for MRTDs including eMRTDs.

Document 9303 is available for free download from the ICAO website. (Use search terms: ICAO Document 9303.)

Document 9303 specifies minimum security features but does not specify which security features must be included in the travel document. Each State should decide, based on risk assessments, which combination of security features meet its security needs.

However, Document 9303 contains recommendations pertaining to 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.

6.5 Types of Travel Documents

It is highly recommended that minimum security features (referred to in the Seventh Edition of Doc 9303, Part 2) 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. Temporary passports may also be issued to meet 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) is available on the Internet. Use search terms: Operational Security Standard on Physical Security

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 (logs created should be kept for possible future investigations). • 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. Where the TDIA shares accommodation with other government departments or agencies, steps should be taken by senior management to ensure that only TDIA employees have access to TDIA areas. 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 but in the absence of these measures, a simple locked door would suffice with a notice to the effect that only authorised staff are allowed entry to the area. Logging of activity (who goes in and out) should be done where possible –even if only with pen and paper - and retained for future possible investigations. 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 and related access rights revoked to avoid the risk linked to potential badge duplication. 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. Visitor badges should only permit access to the rooms/areas the visitor requires access.

- **Escorts**: Visitors should be escorted at all times by a staff member when in restricted zones. This also applies to TDIA employees whose security clearance or position does not allow access to some zones. In fact, special attention should be given to employees with restricted privileges walking in high security zone, as this is much more likely to happen than having a stranger inside a restricted zone.

- **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 and on a system separate from that used for the monitoring to avoid potential loss of records should the monitoring system be compromised.

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. The workflow should have been established considering such catastrophic losses: if anything happens, the personnel should be able to leave the facilities without creating a security issue, for example:

- Blank Documents should be taken from the safe when they are required, instead of taking all blanks required for the day's production at one time, when TDIA employees arrive in the morning. In this way the situation of having many blanks left on the desk if personal have to leave the building hurriedly (without having time to put those blanks back in the safe) is avoided.
- Fire doors and security doors should close automatically and quickly after being opened to avoid the case where an unauthorized person uses or simulates a catastrophic loss to gain access to Security and High Security zones while a TDIA employee is leaving them.

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 and randomly to verify possible internal fraudulent activity.

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. Two-factor authentication systems, if possible, are preferred. All individuals should be limited by access and processing permissions to certain databases, applications and tasks related to their work. Passwords used should be random combinations of alphanumeric characters 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 reauthenticate 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. Even with override, there should be a repository to keep a trace when those overrides occurred, who was authorized to work and if possible the reason associated. Passwords must be changed regularly – every 3 months at the latest- and if possible the IT system should have the facility to require this.

The equipment should have a monitoring and audit trail mechanism to indicate who has accessed the system and which information was consulted. This logging should not be changeable by any users, including administrators. This could be achieved by digitally signing the logs. Moreover, 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, email and social media

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. Moreover, this should be done in accordance with the privacy and data protection laws of the country of the TDIA. All information resulting from monitoring that is not of security interest should be regularly purged from records.

As there is a constant increase in security incidents linked to social engineering, all practices related to this, including but not limited to phishing, baiting or similar social network-based approaches should also be taught to all the TDIA personnel (not only the IT personnel).

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. IT personnel should have access only to the areas/systems which are required for their routine work. In exceptional circumstances an employee may require access to an area/system – to which he normally does not have access. For such cases, a register should be maintained to record access details including who requested access, the purpose, and who authorized the access. This register would serve to provide access details in the case of an investigation into possible fraudulent activity.

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. It can be found on the Internet using search terms: Misconduct Resistance Integration Guide.

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.

Where staff is assigned to a TDIA by a central personnel unit, security/background checks should be already carried out by that unit. However, it is important that TDIA senior management emphasise the importance of proper background checks on staff assigned to the TDIA.

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.

Senior managers should ensure that random checks take place on applications prior to being authorised for issue. Where applications are dealt with on a system, it is possible to include this as a system requirement enabling the system to select applications randomly. Where this has to be done manually, such checks should take place at different times of the day to avoid any obvious pattern.

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. Where a TDIA refers all fraud/suspected fraud case to the police, it is essential that they maintain contact with the investigating authority to track progression of the case and to establish whether there is a need for further analysis of other applications that may also have involved fraud.

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 travel document. 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 travel document 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 travel document 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 and to determine if its loss is in any way a result of fraudulent activity.

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

Examples of public awareness tools on reporting lost and stolen travel documents for different States can be seen on the Internet using the following search terms: reporting lost and stolen travel documents + Country Name [Australia, Canada, New Zealand, United States].

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 travel documents 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 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, refugee travel documents, certificates of identity etc.) 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 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 must 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, stolen, or revoked 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 books and

personalized documents. National databases can assist with the transfer of the required information to the Interpol SLTD.

A central office (usually the National Central Bureau) 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.

A standard data set focusing on the document details rather than the holder of the document has been developed for the interchange of information pertaining to lost, stolen and revoked travel documents. States must meet the following required data fields when uploading to this database:

1. Travel Document Identification Number*;
2. Type of Document (passport or other);
3. Issuing Country's ICAO Code;
4. Status of the Document (i.e. stolen blank); and
5. Country of Theft (only mandatory for stolen blank travel documents).

**Where the travel document has been personalized this should be the number contained in the MRZ; if dealing with a blank book, this number should be the serial number, if the numbers are not the same.*

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.

Fixed Interpol Network Database (FIND) stands for the access to INTERPOL's databases through the 'on-line' integration and communication between an existing national server and IPSG server, via Interpol's communication network.

Mobile Interpol Network Database (MIND) stands for the 'off-line' access to Interpol's databases on the national level for all those countries that, from whatever reason, cannot use FIND.

The Interpol SLTD initiative is widely endorsed by several international fora including ICAO, G8, EU, OSCE (Search Terms; OSCE Decision no 4/04) and the United Nations (Search Terms: Security Council Resolution 1617).

The Regional Movement Alert System (RMAS) is an APEC initiative enabling positive validation of travel documents. RMAS enables participating economies to verify the status of travel documents in

real time at the source, and alert the relevant agencies if action is required. In addition to checking for lost, stolen and invalid travel documents, RMAS is able to determine whether a travel document is recognized by its issuing authority as having been validly issued. (Search Terms: Regional Movement Alert System (RMAS)).

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.

Increasingly, countries are repatriating both personalisation and application processing from overseas. This has the benefit of increasing security across the board but consideration does have to be given to customer service levels, especially where there may be an urgent need to travel.

11.2 Overseeing of Work

In some cases, locally engaged staff carries out issuance functions at missions. It is therefore important that they be thoroughly security screened to the same level as travel document 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/Civil Registration, 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 travel document, 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 travel documents 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/Civil Registration

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)
- Joint Regional Communications Centre (JRCC) of the Caribbean Community (CARICOM)
- 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 travel documents (Chapter 3 of Annex 9 to the Convention on International Civil Aviation). The ICAO Technical Advisory Group on the Traveller Identification Programme (TAG/TRIP) develops and adopts specifications for travel documents which are included in Document 9303. The TAG/TRIP also publishes guidance material and Information Papers to assist States in implementing its specifications. Under the governance of the TAG/TRIP, two working groups operate:

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 Facilitation Section in the ICAO Secretariat should be contacted for any need of assistance related to the issuance of identity and travel documents (e-mail: fal@icao.int).

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 travel document 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 travel documents, the Asia-Pacific Economic Cooperation (APEC) Regional Movement Alert System (RMAS) is able to determine whether a travel document 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, ASEAN 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/

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. *Doc 9303, Machine Readable Travel Documents*
2. *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
3. *Recommended Standards for Secure Proof of Status and Nationality Documents to Facilitate Cross-Border Travel, Security and Prosperity Partnership Deliverable* 1.1.3
4. *A Guide to Biometric Technology in Machine Readable Travel Documents*, APEC Business Mobility Group
5. *G8 Best practice for the processing of travellers who present lost of stolen travel documents*
6. *G8 Best practices on quality control of reporting on lost and stolen travel document data*
7. *Principles and Recommendations for a Vital Statistics System, Revision 2, chapter 3, UN Department of Economic and Social Affairs, Statistics Division, 2001*

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 Technologies 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 and Lost Travel Document Database
TAG	Technical Advisory Group
TDIA	Travel Document Issuing Authority

For Publication on the ICAO Website

Guide for Assessing Security of Handling and Issuance of Travel Documents

Part 2- Assessment Guide

January 2010

File: Guide for Assessing Security of Handling and Issuance of Travel Documents
Author: Subgroup of the Implementation and Capacity Building Working Group (ICBWG), Working group of the ICAO Technical Advisory Group on the Traveller Identification Programme (TAG/TRIP)

Table of Contents – Part 2 Assessment Guide

Instructions for Assessors
How to enter the assessment results in the Assessor's Worksheet (Tab 3) and interpret the risk scoring

1. It is assumed that the assessors will have read Part 1 of the Assessment Guide called, "Best Practices on Secure Issuance of Travel Documents".

2. Tab 3 of this Excel Spreadsheet called "Assessor's Worksheet" is the worksheet where the assessors will enter the results of their assessment of a Travel Document Issuing Authority (TDIA).

3. Each question refers to a specific best practice identified in Part 1 of the Assessment Guide. If a question is not clear the assessor should refer back to Part 1 to get a clearer understanding of the issue being addressed. The applicable section number is listed in the column next to the question number.

4. There are three columns for the assessors to enter their results. These are "Compliance", "Remarks on Gaps and Mitigation Measures", and "Risk". All other columns are shaded to indicate that data cannot be entered in them.

5. **Compliance column:** Indicate on a scale of 0-100 the degree to which the TDIA complies with the question asked. If the answer is a definitive "Yes" the compliance will be 100%. If the answer is "No" the compliance will be 0%. The assessor can indicate the degree of partial compliance by entering a value between 0-100%. If the question is "not applicable" leave this cell blank. See the note at 7 below.

6. **Remarks on Gaps and Mitigations column:** Comments are required whenever the compliance with the best practice is less than 100%. This is the most critical part of the assessment process. The assessor should state the specific way in which the TDIA is not compliant and any mitigation measures in place to lessen the risk for not complying with the best practice. For example, the TDIA may achieve a high level of security through different means. If the question is not applicable or there is no information available, a reason should be given. If the non-compliance is not sufficiently mitigated, the remark should indicate that further review or action should be considered The comments in this column will explain to the TDIA's senior management and to donor states (in the case of capacity building initiatives) why and how determinations of risk have been made.

7. **Risk column:** Use the dropdown menu to indicate whether the level of risk is low, medium or high (L/M/H).

- **Low** means that the TDIA can accept the level of risk or that there is no urgent need to make changes to the TDIA's current practices.
- **Medium** indicates that there is a significant risk but that corrective measures may not be an urgent priority.
- **High** indicates that the risk is serious and that corrective measures should be considered as a priority**.**

Note: For questions that are "not applicable", the risk should be put as "Low". This is because questions that are not applicable are not considered problem areas requiring further attention.

Note: For questions that cannot be answered due to lack of information, the risk should be put as "High". Until there is sufficient data to accurately determine the risk level, unknown risk is considered high risk.

How the risk scoring works

8. Once the assessor enters the TDIA's percentage of compliance and the risk (H/M/L) for each question, the Assessment Guide will automatically calculate a "Risk Score" which indicates which issues present the highest vulnerabilities for the TDIA.

9. The risk score for each question will be between 0-100%. A low score is good. A higher score indicates that further review or changes to a country's practices may be needed. Where compliance is 100% the risk score will be 0%.

10. When the assessor marks the risk as low, the risk score will also be 0% even if there is no compliance with the best practice associated with that question. This is because low risk means that the TDIA can accept the level of risk or that there is no urgent need to make changes to the TDIA's current practices. Where the assessor marks the risk as medium or high, the risk score will be higher. For example, where compliance is 0% and the risk is high, the risk score will be 100%.

11. Low compliance and medium or high risk will generally result in higher risk scores. High compliance and low or medium risk will generally result in lower risk scores.

Note: This guide had been locked to avoid inadvertently changing any of the content. If modifications need to be made click on the review tab, then click "unprotect sheet", the password is "icbwg". Do not forget to protect the sheet in the same way after making necessary changes. However, the High Risk Results sheet should not be password protected as it will not refresh if protected.

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
Chapter 1 - Travel Document Issuing Authority - Organizational Structure, Internal Security and General						
1.2 Organizational Structure						
101	1.2.1	Is the Travel Document Issuing Authority (TDIA) an independent governmental organization (or section) focusing only on the issuance of travel document (and other governmental ID documents)?				
102	1.2.1	Is there only one TDIA responsible for all travel documents issued?				
103	1.2.1	Does the TDIA report to a senior executive level within the government?				
104	1.2.1	Is the TDIA supported by laws and/or regulations?				
105	1.2.1	Are these laws and/or regulations enforced?				
106	1.2.1	Do these laws and/or regulations clearly set out the mandate, responsibilities, and the limits of authority of the TDIA?				
107	1.2.1	Do these laws and/or regulations permit the TDIA to operate independently and carry out its mandate without interference?				
108	1.2.1	Is the TDIA recognized as being an essential component of country security?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
109	1.2.2	No matter the organizational structure used (decentralized/centralized), is there centralized supervision and controls in place for all aspects of the issuance process?				
If the TDIA uses partners (public or private) to carry out some of its issuance functions, please answer the following questions:						
110	1.2.3	Are all entitlement decisions made exclusively by appropriate TDIA staff members?				
111	1.2.3	Are there contracts or memorandum of understanding in place describing all rights and responsibilities or the parties involved?				
112	1.2.3	Does the TDIA perform regular risk assessments, reviews and audits of partners to ensure they have adequate on-site security and safeguards?				
113	1.2.3	Is a Threat and Risk Assessment of the partners conducted prior to engaging them to carry out any issuance functions?				
1.3 Security Framework						
114	1.3.1	Is there a TDIA security team or section that is directly responsible for developing, overseeing, and managing the security framework?				
115	1.3.1	Is this team independent of the operations chain of command?				
116	1.3.1	Does this team include specially-trained security specialists for the various aspects of security?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
117	1.3.1	Does this team make regular reports on its activities to senior management?				
118	1.3.1..1	Is there a senior manager designated at the national level (headquarters) responsible for internal security controls?				
119	1.3.1..1	Is this manager a participant in the planning and decision making levels?				
120	1.3.1..1	Is this manager independent from the operational chain of command?				
121	1.3.1..1	Is there a senior officer designated at each production site (field office) responsible for internal security controls?				
122	1.3.1..1	Are these officers independent of the operational chain of command?				
123	1.3.1..1	Are these officers functions independent of the application and document processing functions?				
124	1.3.1..2	Is there a group specialized in anti-fraud in place at the headquarters and represented in each facility?				
125	1.3.1..2	Does this group liaise with other government entities that produce breeder/primary and supporting documents?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
126	1.3.1..2	Does this group liaise with government agencies that prosecute fraud when it is found?				
127	1.3.2	Is there a security policy framework in place including a comprehensive set of detailed security policies, practices, and guidelines?				
128	1.3.2	Are the security policies, practices and guidelines available in written form?				
129	1.3.2	Does this security framework affect all aspects of TDIA operations?				
130	1.3.2	Are all such security policies and practices also fully and consistently implemented in all facilities and partner organizations that are involved with travel document issuance?				
131	1.3.2	Are the security policies, practices and guidelines communicated to all employees?				
132	1.3.2	Are the security policies, practices and guidelines easy to refer to?				
133	1.3.2	Are the security policies strictly enforced?				
134	1.3.3..1	Is security a recognized high priority of the TDIA in all of its operations and facilities?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
135	1.3.3..1	Does the security framework have strong support from senior management?				
136	1.3.3..2	Is the security framework adequately supported financially?				
137	1.3.4	Does the TDIA use any techniques to establish and maintain a strong “culture of security”?				
138	1.3.4	Is there a security awareness program in place?				
139	1.3.4	Are employees regularly trained on the security policies?				
140	1.3.4	Is the operating environment such that all staff are encouraged to make suggestions on possible improvements to security practices?				
141	1.3.5	Are staff security responsibilities considered an important part of, and included in, their performance assessments?				
142	1.3.6	Does the TDIA regularly forecast work demands and surges in applications, and plan accordingly?				
143	1.3.6	Does the TDIA have constructive plans to deal with increases in demand, excess sickness, and other work overflow situations in order to maintain operations without security compromise?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
144	1.3.6	Does the TDIA maintain a group of pre-cleared background-checked and trained part-time call-up resources to use in case of overload or other under-staffed situations?				
1.4 General Security Practices						
145	1.4.1	Does the security team, or other appointed agency, regularly carry out Threat and Risk Assessments (TRAs) on all TDIA operations, in all facilities, to ensure that security is well implemented and updated?				
146	1.4.2	Does the security team, or other appointed agency, carry out regular audits and reviews to ensure that the security policies are consistently and properly practiced across all operations and offices?				
147	1.4.2	Are some of these reviews and audits unscheduled and carried out on an ad-hoc unannounced basis?				
148	1.4.2..1	Is there a compliance process in place to ensure that needed changes identified by the audits are implemented?				
149	1.4.2..2	Are there external audits carried out regularly?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
Chapter 2 - Application Processes						
2.2 Application Processes and Requirements						
201	2.2.1	Are all applications processed in a uniform and consistent manner throughout the TDIA?				
202	2.2.1	Are the same standardized application forms always used?				
203	2.2.2	Are there clear written policies and practices in place covering all aspects of the application and issuance processes for first time applicants and applications for renewal of travel documents?				
2.3 Photographs						
204	2.3	Are photos taken by a commercial photographer, trusted partners or country official?				
205	2.3	Are only photos which meet ICAO Doc 9303 specifications for photos accepted?				
206	2.3	Are there mechanisms in place to reject unacceptable photos and request new ones?				
If the TDIA accepts digitized photographs, please answer the following questions:						
207	2.3	Are digitized photos taken by trusted partners or country officials?				
208	2.3	Are digitized photos transmitted securely from the point of capture to the TDIA without an opportunity for alteration?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
2.4 Secondary Biometrics						
209	2.4	Is a secondary biometric collected as part of the issuance process?				
2.5 Treatment and Protection of Personal Information						
210	2.5	Is every application logged at first receipt and its status updated throughout the application processing chain?				
211	2.5	Are individuals involved at different stages in the application handling process identified on the status log record?				
212	2.5	Are these individuals “signed off” in some fashion when they pass the application on to the next stage?				
213	2.5	Can every document (or document copy) be accounted for at all times throughout the application process?				
214	2.5	Are ALL physical copies of ANY personal information stored in appropriate locked filing cabinets or protected rooms, except when being securely worked on?				
215	2.5	Are all computerized records protected at all times by the appropriate IT Security standards?				
216	2.5	Is it true that at NO TIME applications containing personal applicant details are stored or shared via unprotected networks or portable devices that can be removed from the travel document facilities, e.g. laptops, memory sticks, discs?				
217	2.5	Is staff restricted from “working out of office” on applications?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
218	2.5	After application processing is completed, are all application materials and personal details of the applicant carefully and securely stored in appropriately locked cabinets and protected rooms, and in appropriate IT security-protected databases?				
219	2.5	Is access to the archived records, whether manual or digitized, also subject to strict “permission” control and access logging and tracking?				
220	2.5	Are appropriate destruction or shredding devices used to destroy any information no longer required?				
221	2.5.1	Have automated passport issuing processes been implemented?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
Chapter 3 - Entitlement Processes						
3.1 Summary						
301	3.1	Are all entitlement decisions made by appropriately trained TDIA staff?				
3.2 Treatment of First Applications versus Renewals						
302	3.2	Are first time applicants given special attention and treatment for identity confirmation and entitlement validation?				
303	3.2	Is the application data submitted in support of a renewal application compared to details of travel documents previously issued to that individual?				
304	3.2	Are there special reviews and scrutiny practices carried out for renewal applications submitted a long time (> two years) after expiry of the previous travel document?				
3.3 Applications for Children						
305	3.3	Are children issued their own passports?				
3.4 Documentary Evidence						
306	3.4	Are two or more trusted breeder and support documents submitted by new applicants?				
307	3.4	Are the breeder and support documents that are accepted official government documents?				
308	3.4	Where possible, are these documents required to contain specified security features and secure photos?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
309	3.4	Are there any special procedures defined for dealing with new applicants possessing limited breeder documentation, e.g. an older paper birth certificate with no photo, an older social security document, no driver's license, etc.?				
310	3.4	Are these breeder and support documents scanned and stored on the applicant's database record for renewals or future reference?				
311	3.4	Are the breeder and support documents retained by the TDIA during the application process and returned to the applicant with the travel document?				
312	3.4	Are these scanned breeder and supporting documents universally used for visual comparison purposes with the renewal application?				
313	3.4	Is the expiring or expired travel document always required for renewal applications?				
314	3.4	Is the old travel document submitted to a detailed electronic and visual comparison to its record on file?				
315	3.4	Are at least two of the physical security features of the old travel document verified forensically?				
316	3.4	If the previous travel document is an ePassport, is the chip information read and validated?				
317	3.4.1..1	Are these documents universally subject to basic forensic review?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
318	3.4.1..1	Are employees receiving applications trained to validate the authenticity of breeder and support documents?				
319	3.4.1..2	Do entitlement officers have access to comprehensive documentation, or databases, containing images and specifications of each kind of breeder or support document accepted?				
320	3.4.1..3	Are these documents regularly verified with the issuing authorities or checked through a shared connection to the databases of the breeder document issuing authorities?				
321	3.4.1..3	Are death records always checked for all applications?				
3.5 Other Means of Identifying Applicants						
322	3.5.1	Where first-time applicants are required to apply in person are they interviewed?				
323	3.5.1	Are interviews conducted where there is doubt regarding the integrity of the information and documentation provided?				
324	3.5.1	For an appearance in person or an interview are the employees receiving the application adequately trained to determine prima facie identity and application validity?				
325	3.5.1	Does this specifically include judgment of personal mannerisms and “confidence” of the applicant, similar to that carried out by trained border officials?				
326	3.5.1	During a personal appearance is the applicant compared to the photo being submitted?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
327	3.5.2	Are guarantors used for first time applications where interviews are not conducted?				
328	3.5.2	Are guarantors members of a recognized association where current address and contact information is maintained and can be verified by the TDIA?				
329	3.5.2	Are they holders of current passports (or other travel documents)?				
330	3.5.2	Are guarantors disqualified if they are paid by the applicant for acting as guarantor?				
331	3.5.2	Is there a clear policy in place against such payments and does it appear on the individual's application form signed by the guarantor?				
332	3.5.2	Are guarantors required to sign and date at least one of the photos submitted by new applicants?				
333	3.5.2	Are such guarantors disqualified if they are closely related to the applicant, e.g. siblings, parents, grandparents, children, uncles and aunts, or step and in-law relationships?				
334	3.5.2	Are guarantors contacted on a regular basis to verify their statement?				
335	3.5.2	Are guarantors contacted when there is doubt about the identity of the applicant?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
336	3.5.3	Are any personal references provided with the application?				
337	3.5.3	Are these references independent and unrelated to the applicant and each other?				
338	3.5.3	Are these references contacted to verify the identity claimed by applicants?				
339	3.5.4	Is the applicant's social footprint verified to confirm a claimed identity?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
Chapter 4 - Treatment of Materials and Blank Books						
4.1 Summary						
401	4.1	Does the TDIA have documented policies and procedures related to the treatment of materials and blank books?				
4.2 Book Production						
402	4.2	Are all materials and blank books stored in high security zones?				
403	4.2	If the travel document is produced by a third party in independent facilities, are the security levels for storage of materials and books also high?				
4.3 Numbering						
404	4.3	Are travel document blanks individually numbered such that each one can be identified at any point in the storage and issuance processes?				
405	4.3	Is the number the same as the travel document number eventually issued?				
406	4.3	Does this number appear on each interior page?				
407	4.3	Is the number printed on or laser-perforated through all interior pages?				
408	4.3	Is each internal page of each travel document numbered in sequence?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
409	4.3	Are page numbers also imprinted with UV ink?				
4.4 Shipping and Storage						
410	4.4	Are travel document blanks stored in highly secure areas, such as a vault or safe, with highly-restricted access?				
411	4.4	Is such access limited to small group of trusted individuals having supervisory authority?				
412	4.4	Is the access controlled using ID cards, biometrics, pass codes, etc.?				
413	4.4	Does this protection include 24-hour guarding of the areas or of the facility overall?				
414	4.4	Are the areas where materials and blanks are stored subject to physical security protection appropriate to the security classification of those assets (see section 7)?				
415	4.4	Does this protection include reasonable safeguards against fire and catastrophic losses?				
416	4.4	Are these storage areas backed up with alternate secure storage locations such that travel document issuance may continue in the event of catastrophic loss?				
417	4.4	Are blank books transported with the equivalent safeguards of the storage area such as by armored vehicle used to transfer cash?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
418	4.4	Do the transmitter and the receiver both have to sign off on batches received?				
419	4.4	Is the assignment of blank books to production staff carried out with a minimum of two authorized individuals (four eyes)?				
420	4.4	Are both employees required to sign for blanks stored and removed from the secure area?				
421	4.4	Are all unused books always returned to the secure area in strictly controlled time periods (such as an individual's work shift)?				
4.5 Accounting						
422	4.5	Are all books tracked, using the inventory control number, from the time they are shipped by the manufacturer to the time they are printed as a travel document or spoiled?				
423	4.5	Are blank books counted by at least two people every time they change hands?				
424	4.5	Are black books counted by at least two people when removed from the safe in the morning and unused books counted at night when returned to the safe at the end of the day or shift?				
425	4.5	Are these records inspected daily or on a shift basis by a third party?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
426	4.5	Are all staff members entrusted with blank books always checked on leaving secure areas to ensure that no blanks have been removed?				
427	4.5	If not, are these checks carried out randomly and frequently?				
4.6 Destruction						
428	4.6	Are all spoiled, defective, or excess blank books destroyed thoroughly in a process witnessed by at least two individuals with access privileges to the storage area?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
Chapter 5 - Personalization and Delivery						
5.2 Personalization						
501	5.2	Is the personalization function carried out in a highly secure area with limited authorized access?				
502	5.2.1	Is the personalized travel document subject to a quality assurance review to ensure there are no mistakes?				
503	5.2.1	Is the MRZ read electronically and compared to the data page and the original application information (database and original forms)?				
504	5.2.1	For an eMRTD, is the chip read and the data (including the image) compared to the data page, the MRZ and the original application information?				
505	5.2.1	Is the Digital Signature verified?				
5.3 Delivery						
506	5.3.1	Are recipients required to pick up their travel document in person?				
507	5.3.1	Is the photo on the travel document data page (and chip in the case of an ePassport) checked against the database and the recipient on pickup?				
508	5.3.1	Is an ID document with picture checked on pickup?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
509	5.3.1	Are any questions regarding address, mother's maiden name, etc. asked at time of pickup to ensure the identity of recipient?				
510	5.3.1	Are any biometrics checked at pickup (facial recognition technology, fingerprints)?				
511	5.3.1	At the time of pickup does the applicant sign a receipt indicating that the travel document has been pickup?				
512	5.3.1	Are third parties prevented from picking up travel documents on behalf of the recipient?				
513	5.3.1	If third parties are permitted to pick up travel documents, do they have to present a signed authorization from the recipient that allows him or her to do this, as well as an ID with photo?				
514	5.3.1	Is the person picking up the travel document required to sign a receipt?				
If some personalized documents are mailed, please answer the following questions:						
515	5.3.2	Are reliable mail services used?				
516	5.3.2	Does the receipt of a travel document by the applicant or others living at the same address require a signature?				
517	5.3.2	If not, are there other means used to track whether an applicant has received his or her travel document (such as return of a code word or receipt)?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
518	5.3.2	Is delivery or pickup time monitored after release of a new travel document and are alerts issued if standard time periods are passed without receipt of such confirmation?				
519	5.3.2	Is confirmation of delivery or pickup entered into the TDIA system as a proactive indicator and recorded as the last stage of the issuance process?				
520	5.3.2	Are undelivered travel documents returned to the TDIA for verification of the address in the database as well as with the applicant?				
521	5.3.2	Are travel documents reported as undelivered handled in the same way as lost/stolen travel documents?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
Chapter 6 - Document Security						
6.2 Machine Readable Travel Documents (MRTD)						
601	6.2	Does the country issue Machine Readable Passports (MRPs) in accordance with ICAO specifications Doc 9303 Part 1, Volume 1?				
6.3 Electronic Machine Readable Travel Documents (eMRTD)						
602	6.3	Does the country issue electronic Machine Readable Passports (eMRPs) in accordance with ICAO specifications Doc 9303 Part 1 Volume 2?				
603	6.3	If not, does the country have a plan and schedule to issue such eMRPs?				
604	6.3	Does the country participate in the ICAO Public Key Directory (PKD)?				
6.4 ICAO Standards, Recommended Practices and Specifications						
605	6.4.1	Are all travel documents issued by the country compliant with ICAO specifications Doc 9303?				
606	6.4.1	Are all travel documents designed with strong modern security features of the sort recommended in the **ICAO Informative Annex to Document 9303 Volume 1 Section III: "*Security Standards for Machine Readable Travel Documents*"?**				
607	6.4.2	Does the TDIA have an ongoing program to review and upgrade security features for its travel documents?				
608	6.4.2	Are all travel documents valid for a maximum of 10 years?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
609	6.4.2	Do all travel documents issued respect the one passport/one person policy?				
6.5 Types of Travel Documents						
610	6.5	Do all travel documents issued by the country include minimum security features?				
611	6.5	Are Diplomatic and Special passports issued with the same blanks or materials (except book cover colour) as the regular passport?				
612	6.5	Do passports issued for single trip purposes (to return to the home country via a certain itinerary) include physical security features to prevent counterfeiting?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
Chapter 7 - Facility Security						
7.2 Physical Security Policies						
701	7.2	Is there a physical security policy in place which covers all facilities and spaces used in the handling and issuance of travel documents?				
702	7.2	Are physical security standards compatible with government standards and guidelines and internationally accepted standards?				
703	7.2	Are all TDIA operations facilities, security and high security zones owned by the government?				
704	7.2	Do the facilities used by public and private partners meet physical security standards set by the TDIA?				
705	7.2	Are staff trained on physical security policies and practices?				
706	7.2	Are there sanctions for staff who do not follow the security policies and practices?				
7.3 Security Zones						
707	7.3	Are the various issuance facilities and work zones defined in terms of different security zones (Public Zone, Reception Zone, Operation Zone, Security and High Security Zones)?				
708	7.3	Are these different zones subject to different levels of physical security protection as appropriate?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
709	7.3	Do they include security practices to be followed for access control?				
710	7.3 &7.4	Do they include security practices to be followed for monitoring and guard requirements for different security zones?				
711	7.3	Do they include additional security practices such as physical construction or protection devices, for different security zones?				
For customer service area						
712	7.3.1	Is the reception area where the public applies for and receives travel documents built so that customers cannot have easy physical access to staff?				
713	7.3.1	Are there additional physical security measures in place such as screening, bullet-proof glass and duress alarm to protect employees?				
714	7.3.1	Are security personnel present during working hours?				
For restricted-access areas (Operation Zone and Security and High Security Zones)						
715	7.3.2	Are access control systems implemented such that access is subject to specific privileges applying to each staff member individually?				
716	7.3.2	Is employee access restricted to certain time periods i.e work shifts?				
717	7.3.3	Do access privileges to security and high-security zones require a two-factor authentication of the individual?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
718	7.3.3	Is the area where books are personalized placed under secure lock down at the end of every business day?				
719	7.3.3	Do access privileges to security and high-security zones require more than one so-privileged person in the zone at all times?				
7.4 Access Control and Monitoring						
720	7.4	Are all site facilities monitored by guards on a 24/7 basis?				
721	7.4	Are employees required to wear access privilege badges at all times?				
722	7.4	Do access privilege badges include clear photos of the bearer?				
723	7.4	Do access privilege badges have colours or other obvious codes to visually indicate the physical privileges of the bearer?				
724	7.4	Are visitors/contractors always escorted in all secure areas?				
725	7.4	Does this apply to employees who do not have the appropriate security clearance or whose position does not give access to certain zones?				
726	7.4	Is physical access controlled by physical and electronic means (locks, access privilege IDs, biometrics etc)?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
727	7.4	Are intrusion detection devices used (alarms, motion sensors, etc.) to trigger immediate attention of the guards?				
728	7.4	Are cameras and CCTV used in all external and internal door entry locations, and internal hallway and room areas?				
729	7.4	Are the video records from the monitoring equipment stored for appropriate periods (more than three months)?				
7.5 Other Physical Security Protection and Practices						
730	7.5	Is all mail, including travel document application and material received screened (X-Ray) in an appropriately located mailroom?				
731	7.5	Are facilities, assets and data protected against fire and other catastrophic losses?				
732	7.5	Are there arrangements in place for alternative sites and backup storage sites to ensure the continuity of operations?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
Chapter 8 - Information Technology Security						
8.2 IT Security Policies and Practices						
801	8.2	Is there a comprehensive IT security policy in place?				
802	8.2	Is this policy up-to-date with regard to current technologies and practices?				
803	8.2	Is this policy implemented and practiced in full for travel document issuance IT systems, databases, and information flow?				
804	8.2	Does this policy refer to and incorporate current international standards such as ISO/IEC 27002:2005?				
805	8.2	Do these policies and practices include risk and vulnerability assessments, IT data privacy assessments, lost of data base information, unauthorized data access, and related assessments?				
806	8.2	Do the IT security policies and practices deal with appropriate **confidentiality** classifications of systems, databases and related information such that this information cannot be accessed, intercepted, or otherwise copied and obtained electronically by the wrong persons?				
807	8.2	Do the IT security policies and practices deal with appropriate **data integrity protection** of systems, databases and related information, such that this information cannot be changed, added to, or deleted except in the properly defined processes?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
808	8.2	Do the IT security policies and practices deal with appropriate **data availability** of databases and related information, such that this information cannot be blocked or hidden from legitimate users when it is required?				
809	8.2	Do the IT security policies and practices deal with appropriate **permissions of access** to systems, databases and related information, such that this information can only be accessed by **the authorized intended users** of the information?				
810	8.2	Have these policies, technologies and methodologies been evaluated by competent professional IT auditors to verify their efficiency and performance?				
811	8.2	Have technology products such as database software packages, servers, communications facilities, hardware security modules (HSMs), and other commercial products that are used, been certified at the appropriate Evaluation Assurance Level (EAL) security level?				
812	8.2	Have the cryptography devices used been certified to the appropriate level using international standards such as FIPS 140-2 or equivalent?				
8.3 User Security						
813	8.3.1	Do all users of the system and databases require at least a unique username and password sign-on in each case of such access?				
814	8.3.1	Are these individuals also limited by access and processing permissions to only certain application processes and to certain database records?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
815	8.3.1	Do all such sign-on sessions automatically terminate after short periods of inactivity?				
816	8.3.1	Can all accesses to the issuance IT system be monitored electronically?				
817	8.3.2	Does the TDIA deny Internet access to staff or contractors from any computer application PC or terminal used in the issuance process?				
818	8.3.2	Are such devices physically and technologically segregated (that is, either used for the application processing or for email and Internet)?				
819	8.3.2	Is there 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 that may be of concern?				
820	8.3.2	Is the process 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, and information that is not of security interest purged from records?				
8.4 IT Personnel						
821	8.4	Do IT personnel with physical access privileges to IT facilities, such as computer equipment rooms, physical databases, and communications facilities, have special access rights for entry to these facilities?				
822	8.4	Do these access privileges involve two-factor identification, such as a biometric measurement as well as a physical access token (such as an ID card)?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
823	8.4	Does access to these computer rooms or other physical IT facilities always require two or more authorized individuals at any time?				
824	8.4	Are IT Personnel responsibilities segregated and clearly defined so that no one individual ever has the right to overrule security policies and practices and make arbitrary decisions, make arbitrary backups of databases and other information files or in any way compromise the issuance system and its confidential information?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
Chapter 9 - Protecting and Promoting Personnel and						
9.2 Security Clearances and Security Briefings						
901	9.2.1	Are all employees and contractors submitted to a background screening and reliability check corresponding to the classification level of the task (position) required?				
902	9.2.1	Are all staff positions assigned a classification or security level designation that recognizes the sensitivity of the position, responsibilities, access, and level of decision-making?				
903	9.2.1	Are these background and reliability checks carried out by or in collaboration with law enforcement, police or national security agencies?				
904	9.2.1	Do background and reliability checks for positions with higher security level classifications include a review of financial history and interviews with friends, family and colleagues?				
905	9.2.1	Are entitlement officers citizens of the issuing country?				
906	9.2.2	Are background and reliability checks repeated at appropriate intervals?				
907	9.2.3	Are secure areas delimited and internal controls in place to limit access authority of employees, both physically and electronically?				
908	9.2.4	Do temporary employees undergo the same background and reliability checks as permanent employees?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
909	9.2.5	Are all staff and contractors provided with an oral security brief and written guidelines on the TDIA's internal controls and security policies?				
910	9.2.5	Are all staff and contractors briefed on their access privileges and prohibitions attached to their security clearance level?				
911	9.2.5	Is there a written code of conduct and/values and/or an ethics code for all employees?				
9.3 Work Organization						
912	9.3.1	Are prescribed job functions established such that one employee cannot perform all the travel document entitlement and issuance functions?				
913	9.3.2	Do office flow procedures prevent the public from being able to select a specific employee?				
914	9.3.2	Are entitlement officers required to take the next batch of work in sequence?				
915	9.3.2	Do staff members rotate through several functions i.e. data entry, open mail etc.?				
916	9.3.3	Are all vital decisions and justifications made during the issuance process recorded in the file and database?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
9.4 Staff Morale						
917	9.4	Overall, has the TDIA implemented modern management principles to encourage a positive and healthy morale amongst all employees?				
918	9.4	Are the employment conditions and the pay structure and benefits for employees fair and competitive for similar work in other local sectors?				
919	9.4	Are there clear Human Resource (HR) policies in effect for employee reviews, pay raises, opportunities for promotions, and other HR matters?				
920	9.4	Are there formal HR mechanisms for employees to file personal treatment grievances and to have these grievances fairly heard and dealt with?				
921	9.4	Is there a high degree of job security at the TDIA for competent employees?				
922	9.4	Are all employees encouraged, with official recognition and other rewards, to make continuing recommendations for security and operational improvements?				
923	9.4	Are stratification conducted and analyzed regulary to 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 Investigations and Sanctions						
924	9.5.1	Are employees regularly reminded of the importance of being on guard and attentive to employee malfeasance and internal fraud including theft of documents, consumables and cash?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
925	9.5.1	Is there a documented policy requirement to have staff report all possible security violations without risk of negative feedback regardless of the nature of the violation or the individual involved?				
926	9.5.1	Are the sources of any such reports kept secret by the TDIA for the protection of reporting staff?				
927	9.5.2	Is there a formal official investigation process to investigate possible serious security breaches by employees at any level?				
928	9.5.3	Is this formal investigation process supported by clear and strong legislation such that offenders can be severely sanctioned if fault is found?				
929	9.5.3	Do these sanctions include immediate firing with loss of all benefits, if appropriate?				
930	9.5.3	Do these sanctions include criminal prosecution, if appropriate?				
931	9.5.3	Are results of investigations well publicized?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
Chapter 10 - Lost and Stolen Travel Documents						
10.2 Prevention Measures						
1001	10.2.1	Are travel document holders made aware of the high security significance of the document and the need to keep it in a safe place?				
1002	10.2.1	Are travel document holders made aware of the importance of immediate reporting of a lost or stolen document?				
1003	10.2.1	Are there easy means of doing so such as well-posted toll-free numbers, fax, online, or in person?				
1004	10.2.1	Is the reporter of a lost or stolen document required to complete a written report?				
1005	10.2.2	Are there important incentives for the holder to take care of his or her travel document, such as: • higher fees for replacements; • requirement to appear in person for reapplication; • personal interview; • a mandatory endorsement identifying the travel document as a replacement; • mandatory hold times; • limited validity period of replacement travel document; • refusal to issue another travel document after a second lost travel document;				
1006	10.2.2	Are there careful entitlement checks done for the production of a replacement travel document?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
1007	10.2.2	In the event of multiple loses, are lost and stolen claims subject to special investigations, including the possibility of a police investigation?				
10.3 Mitigation Measures						
1008	10.3.1	Are lost and stolen travel documents immediately cancelled and declared invalid for travel?				
1009	10.3.1	Do lost and stolen travel documents remain invalid if subsequently found by the rightful holder?				
1010	10.3.1	In this case, are they submitted to the TDIA for physical cancellation or destruction?				
1011	10.3.2	Are the travel document numbers stored in a national Lost and Stolen travel document database?				
1012	10.3.2	Are they so stored for at least as long as the validity period of the document?				
1013	10.3.2	Are lost or stolen blank passports reported in a national Lost and Stolen travel document database?				
1014	10.3.2	Is this database available to border control, immigration, visa, and law enforcement authorities?				
1015	10.3.3..1	Are lost and stolen travel documents reported to the Interpol SLTD?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
1016	10.3.3..1	Are missing blank passports reported to the Interpol SLTD?				
1017	10.3.3..2	Are lost and stolen travel documents also shared with international partners and/or APEC RMAS?				
1018	10.3.3..2	Are missing blank passports reported to international partner and/or APEC?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
Chapter 11 - Overseas Issuance						
11.2 Overseeing of Work						
1101	11.2	Are all overseas consular staff members and locally engaged staff who handle travel documents security screened to the same level as the personnel in the home country?				
1102	11.2	Does overseas staff receive the same training as the personnel in the home country?				
1103	11.2	Are policies, entitlement criteria, application requirements, etc. the same as in the home country?				
1104	1.3.2	Are all security policies and practices also fully and consistently implemented in all facilities and partner organizations that are involved with travel document issuance?				
1105	11.2	Are there constant communications between headquarters and missions to ensure policies and practices are known and applied?				
1106	11.2	Are audits and spot checks performed on a regular basis to ensure that all policies and practices are being enforced overseas?				
11.3 Entitlement						
1107	11.3	Does a supervisor who is a citizen of the issuing country always approve the final entitlement decision?				
1108	11.3	Do the missions have access to the same clearance, watch lists and travel restriction databases as domestic offices?				
1109	11.3	Are any difficult cases referred to headquarters?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
1110	11.3	Are travel documents issued at missions included in national databases?				
11.4 Personalization						
1111	11.4	Are the books personalized overseas with the same personalization (printing) technology and stock, including security features as the books produced in the home country?				
1112	11.4	Do only the officers responsible for travel document issuance have access to blank books?				
1113	11.4	If locally engaged staff is able to personalize travel documents, are these always checked by senior consulate staff who are citizens of the country before release?				
1114	11.4	For travel documents personalized overseas in consulates, are all steps proposed in Chapters 4 and 5 for handling, accounting and storage of blanks also fully implemented in the missions abroad?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
Chapter 12 - National and International Stakeholders						
12.2 National Stakeholders						
1201	12.2	Does the TDIA have active partnerships with other national authorities that are stakeholders in the issuance and use of travel documents?				
1202	12.2.1	Does the TDIA exchange information with border control and immigration authorities on the development, design and integration of security features in travel documents?				
1203	12.2.1	Does the TDIA exchange information with border control and immigration authorities on document fraud and security threats?				
1204	12.2.1	Does the TDIA exchange information with border control and immigration authorities to ensure interoperability with existing and future border systems and infrastructure;				
1205	12.2.1	Does the TDIA, border control and immigration authorities share data to include in watch lists and travel restrictions lists?				
1206	12.2.2	Does the TDIA exchange information with law enforcement, police and forensic document laboratories regarding travel document fraud and security features?				
1207	12.2.3	Does the TDIA exchange information regarding document versions and security features with Vital Statistics organizations issuing breeder/primary and supporting documents used in the entitlement?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
1208	12.2.4	Does the TDIA exchange information with other national organizations involved in the travel document issuance process, e.g. overseas issuance, diplomatic/special/official passport issuance, accepting applications?				
12.3 International Partners						
1209	12.3	Does the TDIA have active partnerships and associations with other nations and international organizations?				
1210	12.3.1	Is the TDIA aware of the role of the ICAO MRTD program?				
1211	12.3.1	Does the TDIA participate in ICAO TAG/MRTD and its working groups (NTWG and ICBWG)?				
1212	12.3.2	Does the TDIA participate in international data exchange networks such as Interpol LSTD, APEC RMAS or others?				
1213	12.3.2	Does the TDIA participate in regional and international partnerships to share data and information and review threats, frauds, counterfeiters, security features and security practices?				
1214	12.3.3	If required, is the TDIA aware of travel document capacity building programs, help, funds and expertise available?				
12.4 Private Partners						
1215	12.4.1	Does the TDIA share information with airlines and associations that verify travel documents to determine the right to board a plane and communicate advance passenger information?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
1216	12.4.2	Does the TDIA share information with ISO and/or private companies to remain aware of latest developments in travel document technologies, systems and processes?				
1217	12.4.2	Does the TDIA undertake regular Requests for Information to remain aware of latest research and innovations?				

High Risk Items Requiring Review

For convenience, all of the responses to the Assessment Guide questions that were identified as high risk are listed below so that the Travel Document Issuing Authority (TDIA) can review them and determine what action it will take. Although these are the highest priority for action, all medium risk responses should also be reviewed.

Once the TDIA has dealt with the high and medium risk items, the low risk items can be reviewed taking into account the assessors' comments on why the risk is low (i.e. due to mitigation measures, not applicable, etc.) to determine whether any changes are required.

Note: To see data from the Assessor's Worksheet you will need to refresh the table. You can do this by clicking on the OPTIONS tab and then the REFRESH tab; by closing excel and re-opening the program; or by right clicking on the column headings below and selecting "refresh".

No.	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score

Potential Problem Areas Identified by High Risk Scores

The purpose of the “Risk Score” is to help Travel Document Issuing Authorities (TDIA’s) identify areas where they may need to review or change their processes to comply with international best practices.

Risk scores are between 0-100%. Low risk scores are good. High risk scores indicate potential problem areas. The High Risk Results on the previous page of this workbook should be addressed first.

The table below includes the average risk scores for the 12 chapters and for each section within these chapters. The table also shows how many low, medium and high risk responses were given for each section and chapter and for the entire assessment. If no risk score is displayed it maybe because all questions in the section were deemed 'not applicable' on the worksheet.

Chapters and Sections	Risk Score	Number of		
		Low	Med	High
Chapter 1 - Travel Document Issuing Authority -		**0**	**0**	**0**
1.2 Organizational Structure		0	0	0
1.3 Security Framework		0	0	0
1.4 General Security Practices		0	0	0
Chapter 2 - Application Processes		**0**	**0**	**0**
2.2 Application Processes and Requirements		0	0	0
2.3 Photographs		0	0	0
2.4 Secondary Biometrics		0	0	0
2.5 Treatment and Protection of Personal Information		0	0	0

Chapters and Sections	Risk Score	Number of		
		Low	Med	High
Chapter 3 - Entitlement Processes		**0**	**0**	**0**
3.1 Summary		0	0	0
3.2 Treatment of First Applications versus Renewals		0	0	0
3.3 Applications for Children		0	0	0
3.4 Documentary Evidence		0	0	0
3.5 Other Means of Identifying Applicants		0	0	0
Chapter 4 - Treatment of Materials and Blank Books		**0**	**0**	**0**
4.1 Summary		0	0	0
4.2 Book Production		0	0	0
4.3 Numbering		0	0	0
4.4 Shipping and Storage		0	0	0
4.5 Accounting		0	0	0
4.6 Destruction		0	0	0
Chapter 5 - Personalization and Delivery		**0**	**0**	**0**
5.2 Personalization		0	0	0
5.3 Delivery		0	0	0
Chapter 6 - Document Security		**0**	**0**	**0**
6.2 Machine Readable Travel Documents (MRTD)		0	0	0
6.3 Electronic Machine Readable Travel Documents (eMRTD)		0	0	0
6.4 ICAO Standards, Recommended Practices and Specifications		0	0	0
6.5 Types of Travel Documents		0	0	0

Chapters and Sections	Risk Score	Number of		
		Low	Med	High
Chapter 7 - Facility Security		**0**	**0**	**0**
7.2 Physical Security Policies		0	0	0
7.3 Security Zones		0	0	0
7.4 Access Control and Monitoring		0	0	0
7.5 Other Physical Security Protection and Practices		0	0	0
Chapter 8 - Information Technology Security		**0**	**0**	**0**
8.2 IT Security Policies and Practices		0	0	0
8.3 User Security		0	0	0
8.4 IT Personnel		0	0	0
Chapter 9 - Protecting and Promoting Personnel and Agency		**0**	**0**	**0**
9.2 Security Clearances and Security Briefings		0	0	0
9.3 Work Organization		0	0	0
9.4 Staff Morale		0	0	0
9.5 Investigations and Sanctions		0	0	0

Chapters and Sections	Risk Score	Number of		
		Low	Med	High
Chapter 10 - Lost and Stolen Travel Documents		**0**	**0**	**0**
10.2 Prevention Measures		0	0	0
10.3 Mitigation Measures		0	0	0
Chapter 11 - Overseas Issuance		**0**	**0**	**0**
11.2 Overseeing of Work		0	0	0
11.3 Entitlement		0	0	0
11.4 Personalization		0	0	0
Chapter 12 - National and International Stakeholders		**0**	**0**	**0**
12.2 National Stakeholders		0	0	0
12.3 International Partners		0	0	0
12.4 Private Partners		0	0	0
Complete Assessment: Chapter 1 to 12		**0**	**0**	**0**

For Publication on the ICAO Website

Guide for Assessing Security of Handling and Issuance of Travel Documents

Part 3 - A Guide for Experts

Version: Release 1

May 2016

File: Guide for Assessing Security of Handling and Issuance of Travel Documents
Author: Subgroup of the Implementation and Capacity Building Working Group (ICBWG), Working group of the ICAO Technical Advisory Group on the Traveller Identification Programme (TAG/TRIP)

Table of Contents – Part 3 A Guide for Experts

Introduction

Part 3 of the Guide for Assessing Security of Handling and Issuance of Travel Documents (The Guide) is intended for use by experienced and qualified assessors of travel document issuance programs.

The ICBWG developed the Guide to assist States to gain a better understanding of possible threats in all aspects of the travel document issuance process and how they can be dealt with. Part 1 contains best practices; Part 2 can be used for self-assessment and has questions which focus on each aspect of travel document issuance. Part 3 is for use by experts.

Part 3 contains a template for each chapter of the Guide which experts can use as a basic reference during in-country assessments. Each template contains a summary of what's important in the chapter as well as a list of specific issues covered in the chapter. Space is provided for notes and recommendations.

Chapter 1 – Travel Document Issuing Authority – Organisational Structure, Internal Security and General Security Practices

Why is this important? Having a clear mandate and transparent legislative authority minimises the risk of political interference. Having clear security policies and independent security, investigative and audit functions together with good internal controls ensures that both internal and external security risks are mitigated.

Consider:

- Legislation supports the effective issuance of travel documents;
- The TDIA has a clear legislative mandate;
- Laws and regulations exist to cover –basic authority to issue, revoke, withhold, cancel and refuse travel documents; who is entitled to a travel document; requirements that must be met; fees; record keeping; access to information; privacy protection; validity period; instructions for use; penalties for abuse, etc.
- Where services are outsourced clear contractual responsibilities are defined;
- There are independent security and anti-fraud functions with supporting policies in place;
- Comprehensive internal controls that cover all functions of the organisation are in place;
- The organisation has sufficient available funding to meet its expected outcomes;
- The organisation has a culture of integrity and staff are aware of risks and appropriately trained;
- There is effective volume and resource forecasting;
- Risk assessments are regularly carried out; and
- Independent internal and external audits are undertaken.

Current Situation:

Strengths:

Weaknesses:

Recommendations:	C/N

C= critical N=non-critical

Chapter 2 – Application Process

Why is this important? To obtain a travel document, applicants must follow a specified application process, including the completion of forms, submission of documentary evidence, submission of photographs, and in some cases secondary biometrics. The information and documentation they provide will enable TDIA employees to determine an applicant's identity, their eligibility to apply and their entitlement 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.

Consider:

- Application forms and supporting guidance is available, accessible and understandable to ensure quality application information;
- A uniform, consistent and auditable application process is in place across the TDIA to ensure transparency and mitigate corruption and malfeasance;
- Well documented policies and procedures provide support for staff making entitlement decisions;
- The application process is well designed in relation to application type (e.g. first-time or renewal), the local environment, and captures appropriate identity information in an effective and secure manner;
- Quality digitized photographs are captured in accordance with Doc 9303 specifications, and the identity is validated appropriately; and
- Personal information (including biometrics) is stored securely, and only authorized individuals are able to access application information.

Current Situation:

Strengths:

Weaknesses:

Recommendations:	C/N

C= critical N=non-critical

Chapter 3 –Entitlement Process

Why is this important

To ensure document integrity three elements need to established as part of the entitlement process: 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. It is critical that establishing identity is carried out to the highest standard to prevent national travel documents being issued to those not entitled to hold them – this includes criminals and terrorists.

Consider:

- The identity checking process is robust in both passport processes and issuance of documents used to obtain a passport;
- Process for first time applications is different form renewals;
- Documentary evidence is used and is reliable;
- Steps are taken to verify that information is accurate;
- Interviews are used to establish identity – this should also involve the scope for use of social footprint data;
- Existing passport database records are used;
- Staff (including those in agencies issuing supporting documents that may be presented as part of the travel document application process) are trained in detecting forged documents.
- Biometrics, if collected, are checked against other biometric databases (subject to legal permission to do so).

Current Situation:

Strengths:

Weaknesses:

Recommendations:	C/N

C= critical N=non-critical

Chapter 4 – Protection and Secure Management of Raw Materials and Blank Books

Why is this important? Raw materials and blank books must be securely stored, transported and accounted for at all times. Lost and stolen materials and books can be used to create counterfeit personalized documents and can thus negatively impact the reputation of the documents and jeopardize security.

Consider:

- Stock control policies and procedures are documented;
- Storage of blank documents at the production site and the TDIA is secure and transport between these sites is secure. (e.g. limited access vault, armored vehicle etc.);
- Stock manifests are used when stock is moved between sites;
- A unique, unalterable book number appears on each page of the TD (for tracking, mitigating book alteration or use of pages in a new document);
- All raw materials and books are accounted for at all times, including at manufacturing facilities, at the TDIA and between these sites;
- Book usage is accounted for on at least a daily basis(by two people) and more frequently if different staff have custody of books for personalisation purposes. The number of staff who have access to blank books should be limited;
- There should be a separation of duties for those responsible for book custody and control and those staff responsible for book personalisation;
- Waste material and spoiled books are destroyed on a regular basis;
- Books that have been lost by the holder and recovered by the TDIA are recorded and destroyed under supervision.

Current Situation:

Strengths:

Weaknesses:

Recommendations:	C/N

C= critical N=non-critical

Chapter 5 – Personalization and Delivery

Why is this important?
Once the blank booklet has been personalized and delivered, the holder can start travelling with it. Any errors during the personalization process could have a negative impact on the holder in the form of increased scrutiny by border officials. The delivery process should ensure that only the rightful holder obtains the document, to mitigate the risk of use by an impostor.

Consider:

- The personalization premises are secure (access control, intrusion detection);
- Access to the machines, blank books and production batches is controlled and secure (logging, 4-eyes control, random batch assignment);
- Quality checks of the personalized book are conducted (consistency between VIZ, MRZ and chip data, readability of MRZ and chip with appropriate readers, expiry dates, integrity of signature);
- Proper processes and identification checks are in place for in-person pick-ups, either by the applicant or a third party;
- A system is in place for handling unclaimed documents (monitoring, destruction after a reasonable period of time);
- The mailing services used is reliable and receipt of the travel document is confirmed (if travel document is mailed); and
- A system is in place for handling of non-delivery reports (investigations, voiding of validity through lost and stolen databases).

Current Situation:

Strengths:

Weaknesses:

Recommendations:	C/N

C= critical N=non-critical

Chapter 6 – Document Security

Why is this important? Security features are necessary to prevent alterations and counterfeiting of travel documents. Compliance to Doc 9303 specifications for both MRTDs and e-MRTDs ensures interoperability and enhances security.

Consider:

- Compliance to Doc 9303.
- Guidelines on minimum security features implemented.
- Risk based approach to document design and regular review.
- Identical security features across all travel documents including single trip documents.
- One passport/one person policy.

(Reference – Part 1 Chapter 6)

Current Situation:

Strengths:

Weaknesses:

Recommendations:	C/N

C= critical N=non-critical

Chapter 7 – Facility Security

Why is this important? Security of the facilities used to produce the travel document and the personnel involved in the process of issuance must be ensured.

Consider:

- Risk Assessment based on international standards like 27001.
- Risk mitigation and treatment plan with documented security policy.
- Organization wide understanding and awareness of the security policy.
- Minimum controls like
    - segregation of duties,
    - access control,
    - segmentation of work areas and IT facility based on level of security requirement,
    - monitoring of premises and processes,
    - auditable logging of actions,
    - traceability of transactions,
    - protection from fire and other catastrophic losses,
    - business continuity and Disaster Recovery planning

Current Situation:

Strengths:

Weaknesses:

Recommendations:	C/N

C= critical N=non-critical

Chapter 8 – Information Technology Security

Why is this important? The confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information must be safeguarded at all times. Any breach can be exploited to either insert fraudulent data or may lead to loss of personal information collected.

Consider:

- Existence of independently audited IT Security policy and practices in line with 27002.
- Continuous monitoring of vulnerabilities and new threat vectors and appropriate treatment plans with dedicated personnel assigned to this task.
- Segregation of networks
- Systems dedicated to specific functions e.g. System used in issuance process not used for emails, internet surfing.
- Auditable logging of all transactions.
- Segregation of duties (need to know basis) and dual control principals.
- Dual factor authentication for physical access to IT facilities.

(Reference – Part 1 Chapter 8)

Current Situation:

Strengths:

Weaknesses:

Recommendations:	C/N

C= critical N=non-critical

Chapter 9 – Protecting and Promoting Personnel and Agency Integrity

Why is this important? 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. Suspected or detected fraud needs to be investigated and possible sanctions must be in place.

Consider:

- Employees (including temporary employees and contractors) are subjected to background and reliability checks commiserate with their level of responsibility to gauge loyalty, dependability and trustworthiness.
- Security checks are redone regularly.
- Staff is briefed regularly on security policies and is familiar with the code of conduct, values and ethics.
- Tasks are segregated and work randomly distributed to avoid opportunity to commit fraud.
- Vital decisions in the issuance process are logged.
- Management is aware of employee job satisfaction which affects morale and loyalty and knows what action to take if morale is low.
- Employees are required to report security incidents, negligence and misconduct.
- Procedures on incident reporting, investigations and sanctions are documented and known.

Current Situation:

Strengths:

Weaknesses:

Recommendations:	C/N

C= critical N=non-critical

Chapter 10 – Lost and Stolen Travel Documents

Why is this important?
Misuse of genuine travel documents obtained in unlawful circumstances creates serious national security risk. Whether altered or left intact and used by an imposter, these documents can, if undetected, enable terrorist, criminals and irregular migrants to travel virtually unidentified.

Consider:

- Steps are taken to create public awareness (i.e. encourage document holders to safeguard their travel documents, immediately report a missing travel document, etc.);
- Processes are in place for reporting of lost or stolen travel documents;
- Stricter policies are applied to applications submitted by those who have reported their document as lost or stolen;
- Steps are taken to cancel lost or stolen travel documents;
- Data on lost and stolen travel documents is carefully entered into national and international databases (i.e. INTERPOL Lost and Stolen Database, etc.); and
- Effective quality control mechanisms are in place to ensure accurate data entry of information on lost and stolen travel documents (inaccurate entries can result in significant challenges for legitimate travelers).

Current Situation:

Strengths:

Weaknesses:

Recommendations:	C/N

C= critical N=non-critical

Chapter 11 – Overseas Issuance

Why is this important? Whilst overseas issuance forms a small part of overall production it is essential to maintain controls in all areas of the issuance process which at minimum match those in domestic production. Whether entitlement is repatriated or not, headquarters should oversee the work to ensure security best practices are followed at all times.

The following considerations will depend on whether entitlement and production is done locally or not.

Consider:

- Local staff are security screened at the same level as domestic;
- Activities are monitored at the same level as domestic;
- Training, guidance material and access to guidance material is same as domestic;
- Effective and constant communications exists between HQ and mission;
- Citizen of country approves work done by locally engaged staff;
- Misson staff have ability to send difficult applications to HQ;
- Travel Documents issued overseas are included in national database;
- Overseas personalization technology and stock should be the same as used domestically;
- Controls over blank books are tight

Current Situation:

Strengths:

Weaknesses:

Recommendations:	C/N

C= critical N=non-critical

Chapter 12 – National and International Stakeholders

Why is this important? Documents issued by the TDIA are used and verified by national and international stakeholders. They may also assist with the security of the documents and issuing process. TDIA must consult and/or remain in contact with them.
Consider links with:

- Border control and immigration: providing assistance on document design, advice on practical use of security features, fraud trends. TDIA provide border control and immigration with document travel document updates, lost and stolen data, cancellation lists, method to validate data.
- Law enforcement, police and forensic laboratories: assist TDIA with security threats and fraud trends. Investigate TD fraud and counterfeit techniques. Feed data to watch lists and travel restriction lists for use during TD entitlement process.
- Source document, civil registration or vital statistics providers: reciprocal communication exists for document versions, fraud information and verification of both source and travel documents
- Other national authorities & partners: links to others who contribute to watch lists or travel restriction lists. Those who contribute to overseas issuance. Organizations and businesses who use travel documents need to be aware of document, policy or process changes that may affect them.
- ICAO: for Document 9303; for developments coming out of and feeding into the work of working groups; for support with implementing TD programmes.
- Regional groups which may assist with TD implementation, counter-terrorism and general capacity building. There may also be border or TD design agreements to work with.
- Interpol database of lost and stolen upload and download, where applicable.
- Other data sharing arrangements with international partners, whether multilateral or bilateral.
- International private partners, such as airlines, IATA and document verification providers need to be kept abreast of document or policy changes.
- Private companies and groups, such as ISO, evolve new technologies, systems and processes that TDIA should maintain awareness of.

Current Situation:

Strengths:

Weaknesses:

Recommendations:	C/N

C= critical N=non-critical