International Civil Aviation Organization

WORKING PAPER

TAG-MRTD/18-WP/4
22/4/08
English only

# TECHNICAL ADVISORY GROUP ON MACHINE READABLE TRAVEL DOCUMENTS (TAG-MRTD)

**EIGHTEENTH MEETING**

**Montréal, 5 to 8 May 2008**

**Agenda Item 1: Activities of the NTWG**
**Agenda Item 1.4: Guide for Assessing Security Standards for Handling & Issuance of Travel Documents**

# GUIDE FOR ASSESSING SECURITY STANDARDS FOR HANDLING AND ISSUANCE OF TRAVEL DOCUMENTS

Presented by the New Technologies Working Group (NTWG)

## 1. INTRODUCTION

1.1 At TAG-MRTD/17 held in Montréal from 20 to 22 March 2007, WP/19 introduced a project to support efforts to increase the security of the handling and issuance process for travel documents.

1.2 The TAG recognized the importance of increasing the security of travel document issuance and handling, and approved the development of guidelines for assessing the implementation of security standards and best practices in these fields.

1.3 This Working Paper informs the TAG about the progress made to date in drafting the guide and the next steps.

## 2. BACKGROUND

2.1 In recent years, the rapid development of new technologies, most notably the ePassport, has led to the introduction of increasingly secure travel documents. More emphasis is now being placed on the security of the handling and issuance process to help prevent the issuance of legitimate documents to terrorists or criminals under false identities.

2.2 In 2002, members of the Migration Experts Sub-Group of the G8 Lyon/Roma Anti-Crime and Terrorism Group developed a document called ‘Minimum Security Standards For The Handling and Issuance Of Machine Readable (and other) Passports’. This document was then adopted by ICAO as an

Informative Appendix to Section III of Document 9303 Part 1. The Appendix provides a detailed overview of preventing fraud in the application, adjudication, issuance and delivery processes, focussing mostly on internal fraud.

2.3 Worldwide, several capacity building activities are taking place to help countries not yet issuing Machine Readable Passports (MRPs) to meet the ICAO deadline of April 2010. At the same time, many countries are reviewing the security of their own passport issuance process, as they deploy their ePassport program, or just as a regular self-assessment procedure. To this effect, each organization develops its own evaluation tools and techniques.

2.4 Several stakeholders, including States and international organizations, have expressed interest for a common and very practical guidance tool that would help them to either self-assess or assist in evaluation of another country's passport issuance system.

2.5 Hence the purpose of the guide, which includes two sections. The first section actualizes and expands the information from the Informative Appendix to 9303. It recommends best practices to mitigate security threats to every steps of the passport issuance process. The second section provides a comprehensive evaluation tool [checklist] to assess the issuance process vulnerabilities.

## 3. PROGRESS TO DATE AND NEXT STEPS

3.1 An outline of the guide and a draft of the first section were developed using the Informative Appendix to 9303. The draft was presented to the NTWG in Christchurch, New Zealand and was well received by the participants.

3.2 NTWG participants recommended generalizing the guide to ensure it could be used internationally to evaluate different types of systems and organizations.

3.3 The next steps include the completion of the analysis of the first section and continue development of the assessment tool that will constitute the second section.

## 4. ACTION BY THE TAG

4.1 The NTWG invites the TAG/MRTD:

a) to note the work done to date on the Guide for Assessing Security Standards for Handling and Issuance of Travel Documents;
b) to approve continuation of the on-going development of the guide.

— — — — — — —

## APPENDIX

# ICAO Guide for Assessing Security Standards for Handling and Issuance of Travel Documents

Version – 1.3
Date – April 10, 2008

Presented by the New Technologies Working Group (NTWG)

Document Change Control Table

| Version Number | Date of Issue | Brief description of change(s) |
|---|---|---|
| 1.1 | Jan 07, 2008 | 1$^{st}$ draft |
| 1.2 | Jan 18, 2008 | Structure modifications/editing – released to NTWG |
| 1.3 | April 10, 2008 | Produced after NTWG Christchurch discussions |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# Table of Content

# 1 Introduction

## *1.1 Passports role in national and international security*

Passports are official documents that show the identity and citizenship of a person for the purpose of facilitating travel abroad. Border and migration authorities are using them to help determine admissibility and legitimacy of travellers to cross international borders and enter their country's territory. It is also used by the issuing nation to grant re-entry into the country. In addition, passports are increasingly used as identity documents for other types of transactions with government and private sector such as opening bank accounts or accessing governmental services and benefits. As such, the integrity of passports and other travel documents is an important component of national and international anti-crime and anti-terrorism strategies.

Passports, properly obtained or not, altered, or counterfeit, are great tools for criminal and terrorist groups. It enables terrorists to travel to recruit, network, mobilize and organize internationally. Without a passport and the ability to travel freely, terrorists are impeded, localized, possibly even 'quarantined', and their reach and impact impaired. In some cases, a passport may be the only missing key to allow terrorists to reach their final target. Criminal hands are also misusing passports to facilitate illegal migration as well as people smuggling, and human and goods trafficking.

To deliver passports, issuing organizations are processing and storing vast quantities of applicant's personal information. This information needs to be safeguarded as criminals could use it for identity thief or other types of identity frauds. These types of fraud are more and more frequent, and become a great concern of our societies.

Some people and organizations are willing to pay large sums of money to obtain passports illegally, as well as to have access to personal information. It means that the integrity of the travel document and of its issuance process is very vulnerable to fraud and malfeasance. Controlling the security of its documents and its passport issuance process has a direct impact on national security but also on the international respect accorded the documents presented by its citizens for visas and for border crossing, and the entry requirements requested from other nations. Security and reputation of the passport can have serious repercussions on the convenience and expediency of international border crossing for citizens of a country.

While it is acknowledged that passport security is necessary for national and international security, it is also important to recognize that it does remain a great challenge for issuance agencies to find the balance between service, privacy and security.

With the recent fast-paced technological developments, the travel documents themselves become more and more secure against counterfeiting and alterations. More secure documents lead to a shift of focus by fraudsters from counterfeiting and altering passports to obtaining genuine documents by fraudulent means. Therefore, an increased emphasis is now being placed on the security of the handling and issuance process to help prevent the issuance of legitimate documents to terrorists or criminals under false identities. A country can have a highly secure passport document, but if it is being issued to people who are not entitled to have it, the quality of the passport matters very little.

It is now usually recognized that the passport issuance systems **will** be targeted. While it is impossible to eliminate 100% of threats and vulnerabilities, a combination of various features and methods can mitigate them to an acceptable level and deter potential criminal interest. This guide is a tool to inform organizations involved in the passport issuance process about secure best practices. It also provides a tool to help them evaluate the vulnerabilities of their own passport handling and issuance process, or the process of other organizations.

## *1.2 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 specifications and best practices for the issuance of passports and other travel documents, among numerous other responsibilities associated with global air travel matters[1].

The work of ICAO on standardization of travel document commenced in 1968 when a Panel on Passport Cards was established and charged with developing recommendations for a passport book or card that would be Machine Readable. In 1980, the specifications and guidance material developed by the Panel were published as the first edition of Document 9303, '*A Passport with Machine Reading Capability*'.

In 1984, the Secretary General of ICAO established the Technical Advisory Group on Machine Readable Travel Document (TAG/MRTD), made up of experts from several ICAO Member States, to assist in the writing of the specifications for MRTDs. TAG/MRTD develops and adopts specifications for the design of MRTDs, which are published by ICAO in Document 9303. It also publishes guidance material to assist States in implementing its specifications, as well as Technical Reports and Information Papers.

Under the governance of the TAG/MRTD, the New Technologies Working Group (NTWG), in partnership with the International Organization for Standardization (ISO), develops strategies, policies and guidance material related to the manufacture, security, testing, issuance, deployment and globally interoperable use of MRTDs in both physical and electronic form. Another working group, the Universal Implementation of Machine Readable Travel Document (UIMRTD) was also established to support the ICAO Secretariat in carrying out capacity building outreach activities to help ICAO Member States issuing MRTDs and improving security of their issuance process.

[1] MRTDs History, Implementation, and Interoperability

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, endorsed, and assigned to the NTWG.

## 1.3 Purpose

Standard 3.8 of Chicago Convention Annex 9:

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

Several stakeholders, including States and international organizations, have expressed interest for a shared and very practical guidance tool that would help them to either self-assess or evaluate the security of the passport issuance system of another country.

Hence the purpose of this guide, to provide a complete and simple guidance tool for organizations involved in the issuance and management of passports. At first, this guide presents security best practices and recommendations to mitigate security threats to every step of the passport issuance process. Then it provides a comprehensive evaluation tool [checklist and evaluation scale] for organizations to identify their vulnerabilities, or to assess the passport issuance process of others.

Several national and international organizations such as the UN, ICAO, ISO, G8, OSCE, EU, APEC and others have been actively involved in enhancing security of passports and other travel documents. Several regional and international agreements assert the importance for States of ensuring the integrity of their travel documents. Outreach and capacity building activities are taking place worldwide to help countries implement these agreements. NTWG recognizes the work of these organizations and this guide is taking stock of their activities and realizations.

In particular, in 2004 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 them adopted as Informative Annex III to Section III of Document 9303. This valuable document, addressing primarily internal fraud, is the basis for the present guide.

## 1.4 Target Audience

This guide is meant to:

- guide policymakers of organizations issuing and/or involved in the management of passports, to evaluate their own situation;

- support the ICAO UIMRTD and other international organizations and States for outreach, capacity building assistance, or audit purposes;
- assist governments evaluate other States (i.e. States under consideration for visa-waiver eligibility).

These practices apply to both to government and non-government organizations and facilities involved in all stages of the passport issuance process. It is to be used by all types or structure of organizations, internationally.

The measures and practices exposed in this document are recommended practices, and as such, no country is required to adopt any or all. 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.

## *1.5 Scope*

This guide provides best practices and recommendations related to the issuance process for Machine Readable Passports (MRPs) and e-Passports. Most of these are equally applicable to non-MRPs and other travel documents.

This guide addresses primarily the first step of the passport life cycle: the passport issuance process. The issuance process incorporates the decision-making and business processes to establish an individual's identity, citizenship and travel restrictions; produce and deliver a document. It should be noted that the measures taken to enhance the security of the issuance process might also have a direct or indirect impact on other steps of the passport life cycle such as the authentication, the validation and the repudiation.

## *1.6 Structure of Report*

**Part 1 – Best Practices on Secure Issuance of Passports** actualizes and expands the information from the Informative Annex III to Section III of Document 9303. It recommends best practices to mitigate security threats to every steps of the passport issuance process. The first section is divided in ten volumes:

1- Passport Issuing Organization
2- Overseas Delivery
3- Document Security
4- Personnel
5- Physical Security
6- Treatment of Blank Passports
7- Application and Entitlement Decision
8- Treatment of Personalized Document and Delivery
9- Lost and Stolen Passports
10- National and International Stakeholders

**Part 2 – Assessment Guide** provides a comprehensive evaluation tool [checklist and evaluation scale] to assess the issuance process vulnerabilities.

# PART 1: BEST PRACTICES ON SECURE ISSUANCE OF PASSPORTS

1- Passport Issuing Organization
2- Overseas Delivery
3- Document Security
4- Personnel
5- Physical Security
6- Treatment of Blank Passports
7- Application and Entitlement Decision
8- Treatment of Personalized Document and Delivery
9- Lost and Stolen Passports
10- National and International Stakeholders

# 1 Passport Issuing Organization

A first step in ensuring that the passport issuance process is secure is making sure that the organization overseeing the process has the tools to actually carry out its security responsibilities. This means that the organization has the mandate to issue passport, and the legislative framework and the authority to manage the security components of the process. It also means that the organizational type and structure supports its security responsibilities.

It is also crucial that the organizational environment be supportive of the security program implemented. Policies and practices should be in place and supported by management. The effectiveness of these security policies and measures is directly related to the support and priority given by the management.

## *1.1 Mandate and responsibilities*

The passport issuing authority oversees the reception and processing of applications, determination of eligibility of applicants, production and issuance of passports.

Laws are needed to establish the passport issuing authority and the scope and limits of authority of both senior officials and their staffs. Areas for legislation include basic authority to issue, [perhaps also to revoke, withhold, recover] passports, the requirements that must be met by applicants who wishes to obtain the document, fees for the services provided by the issuance authority, record keeping requirements, privacy protections, instructions on the use of passports, and penalties for overstepping one’s authorities.

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 some flexibility. This is good because it sets boundaries for what the applicant can expect to receive, and what staff members can provide on their own authority. It also sets boundaries on what the passport authority can provide when requested to give special handling to applicants or cases referred by political authority.

## *1.2 Organizational structure*

### Security team

In all issuing organizations, there should be a team responsible for security matters. This group ensures the integrity of the passport issuance process, the security and quality of the passport concept and its compliance with governmental security policies and legislations. It is also responsible to define security strategies and policies and develop security training and awareness programs. The individuals who have specific security duties should receive appropriate resources and up to date training.

## Centralized and decentralized Issuance

There are benefits and negatives to both centralized and decentralized issuance processes. Each government needs to come to its own conclusion as of the most appropriate structure, based upon considerations of workload, geography, customer service, etc. Whatever the organizational structure in place, the importance is that mitigation measures be implemented to address the negatives linked to this configuration.

Centralization of passport issuance operations reduces the number of places that have blank passports, the physical security requirements and costs for the system. It also facilitates the control and homogeny of issuance policies and procedures.

Central government officials should supervise decentralization of issuance and produce instructions and documentations to each issuance facility. Adjudication and issuance procedures should be as uniform throughout the system as possible to promote uniformity and consistency in the final document. When a major change is made in the issuance system, it should be made system-wide and simultaneously if possible. There should be a consolidated central database of documents issued and in process.

## In house or outsourcing

The passport issuance organization has to determine whether some of its services, such as book production [or material used in book production], and printing should be done in-house, or by the government, or outsource that particular service to an outside vendor. Several elements should be taken in considerations:

- Costs and resources
- Control of data, material and processes (outsourcing proves less desirable from a control perspective)
- Location, nationality of outsourced companies (political, economic and security context should be taken in consideration)
- Transportation concerns
- Security measures implemented
- Etc.

The issuing authority should conduct reviews of partners and assure that the passport materials and fabrication facilities have adequate on-site security. Environment scans and threat/risk assessments on all facilities are recommended. Secure shipping of passport blanks and consumables by the company producing them, and receipt and accounting for the passports by the issuing authority also need to be closely monitored. Contracts should be in place describing all rights and responsibilities of the parties involved, and penalties if these are not respected.

Before the state begins to tender for a new travel document 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 first - planning phase of the project and pre-project research.

A good practice is to proceed with a Request for Information (RFI) to establish ‘what is out there’ to better determine the needs of the organization.

## *1.3 Management and financial support*

No internal/issuance security system can work properly without support by the head of the passport organization and senior staff. Simply put, decision makers must be willing to commit resources and time for the development, implementation and maintenance of an effective internal controls system. This may require such things as reorganizing workflow, changes in personnel administration, revising other aspects of operations, organization of training and awareness sessions, and use of positive [or negative] reinforcement.

Management must also set the example by following security policies, not break the rules or ask for special favors for people not entitled to them.

It must also be recognized that monetary resources are also required to protect the integrity of the passport and its issuance process, and this can pose difficulties to an issuing authority that operates on a small budget. However it is important to realize that the failure to spend the money needed to have an effective internal controls process can have major costs. They include (but are not limited to) the potential for embarrassment should a country’s passport(s) be used in committing terrorist acts, the difficulties that a country’s citizens will have in international travel if their passports 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 passport fraud. A high quality document issued with a high level of integrity will go a long way to prevent these types of abuse, and the costs of preventing these events through a highly secure issuance process are generally much less than the costs of dealing with the results of an insecure issuance process.

It is for this reason that it is recommended that the process for setting fees for passport services should somehow take account of the actual costs of providing passport services, including the costs of security in all its forms. In this way, the costs of good internal controls become part of the overall cost of the document to the citizen. This is appropriate because the individual citizen benefits most from carrying a highly respected international travel document.

## *1.4 Security policies*

Policies can be defined as a plan or course of action intended to influence and determine decisions, actions, and other matters[2]. Security policies define the strategies, the rules and the practices to follow to reach the security objectives of the organization. Policies help ensuring compliance and consistency of security practices in the organization.

Security policies should be developed in consultation with all stakeholders to get buy-in. They should be easy to understand and easy to follow. Policies should be communicated to all so they are well known and easy to refer to.

One really important policy for the organization is the development of Standards of Conduct or a Code of Values and Ethics. This guide communicates the actions and comportments that are viewed acceptable or unacceptable by the organization. It also includes specific conflicts 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 passport applicants for performing their normal tasks, or in expectation of special favours.

## *1.5 Security culture*

The organization needs to sell security of its staff. The organizational culture should be conducive to the implementation of security policies and practices. Several techniques could be used by senior management to develop a security culture within the organization.

The following are some examples:

- Development of a code of conducts/ values and ethics guidelines
- Regular security training and awareness program and regularly remind individuals of security responsibilities, issues and concerns.
- Communication and advertising campaign on security policies.
- Publish results of security assessments and audits.
- Positive reinforcement and reward good security practices.
- Negative reinforcement and take disciplinary actions for non-compliant or negligent behaviour.

## *1.6 Workload anticipation*

TO COMPLETE - Importance of forecasting and implementing measures to avoid backlogs. Should not increase capacity too quickly.

Internal controls are more important than ever when there is an increased workload because staff concerned with backlogs of applications may be tempted to cut corners or ignore internal controls procedures that may be seen by some as slowing the movement of the work.  Managers must resist the impulse to ignore internal controls.

[2] American Heritage Dictionary of the English language

## *1.7 Environmental scans and threat/risk Assessments*

Regular environment scans and threats/risk assessments are important as they help determine current threats to the system and which assets/areas are most at risk within a process. It leads to recommendations for mitigation measures and safeguards that will reduce risks to acceptable levels.

Organizations should conduct ongoing assessments of threats and risks to determine the necessity of safeguards beyond baseline levels. They 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.

Threat/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.
- Implementing any supplementary safeguards to reduce the risk to an acceptable level.

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 vulnerabilities.  There should be appropriate recognition for those who identify problems, and there should not be reprisals against those who report something as a problem through misunderstanding.

## 2 Overseas delivery

Passports issued abroad are usually issued in much smaller quantity than domestically issued passports, and are often under the jurisdiction of a different department of government than those issued domestically. Despite this fact, it is important that the entitlement criteria, documentary evidence of citizenship and identity, and the document itself, should be as much like the domestic model as possible.

To ensure uniformity of the entitlement process and production of passport, some countries decide to repatriate on or both of these functions to their headquarters. Of course this lengthen the time require for the issuance and deliverance of passports.

Since often the locally-engaged staff do some of the work at foreign service posts, it is important that they be thoroughly security screened, and their activities in the issuance process monitored at least as much as is done with domestic employees. Consular staff should provide the final authorization of passports entitlement decision.

Foreign Service posts issuing passports should have on-line access to the same clearance database as domestic offices, and to the centralized databases. The passports issued by consular posts and diplomatic missions should be included in the database.

Control of blank passport books needs to be even tighter than at domestic facilities. Passport blanks are to be kept in the secure area of the mission and only the officers responsible for passport issuance should have access to the blanks.

# 3 Document Security

Document security refers to the elements incorporated into the physical document to protect it from fraudulent use. These features are to ensure that the information the document contains cannot be easily altered or that deceptive counterfeit documents cannot be easily produced. It includes features that are incorporated at the time of production (e.g. colour shifting inks, steganography, optically variable devices, tactile element, covert feature) or at the time of document personalization (i.e. digital photo of holder, formatting, font, expiry date)

Document security has already been the subject of numerous publications and therefore will not be covered extensively in the present document. However, because it is an integral and major part of the security framework of a passport issuance agency, it seemed necessary to provide an overview of the basics, and mention references that provide details on this subject.

## *3.1 Types of passport*

Two major developments in the recent history of passports contributed to increase significantly the security of the travel document: the development and the worldwide adoption of Machine Readable Passports (MRPs), and of e-Passports.

**Machine Readable Passports**

The MRP is a passport 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-B (OCR-B) style[3]. Document 9303 Part 1, Volume 1 includes specifications pertaining to MRPs.

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

Global interoperability advantages, and security gains brought by MRPs to combat passport frauds, let to the adoption of an ICAO standard to persuade all ICAO Member States to start issuing only MRPs and gradually remove non-MRPs still in circulation.

[3] APEC Document page 3 http://mrtd.icao.int/content/view/18/199/
http://www.dhs.gov/xtrvlsec/programs/content_multi_image_0021.shtm

Standard 3.10 of Chicago Convention Annex 9:

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

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

The Universal Implementation of Machine Readable Travel Document (UIMRTD) Working Group was established to assist the ICAO Secretariat in performing capacity building outreach activities to meet the 2010 deadline.

**E-Passports**

The work of the TAG/MRTD and the New Technologies Working Group (NTWG) since 1998 led to the development of a new generation of passports, the e-Passport. The e-Passport is a type of MRP with an embedded microchip that contains data printed on the data page of the passport, including biographic and biometric information of the holder, and passport data. The chip also contains security features for preventing passport fraud and forgery and misuse of data stored on the chip[4] Document 9303 Part 1, Volume 2 includes specifications pertaining to e-Passports.

E-Passport represents the greatest improvement in travel document security since MRPs as it improves integrity of passports by the need to match the information contained in the chip to the one printed in the document and to the physical characteristics of the holders; and it enables machine assisted verification of biometric and biographical information to confirm the identity of travellers.

Although they will not be the answer to all passport fraud on their own, e-Passports offer greater protection against fraudulent misuse and tampering and reduce the risk of identity fraud at border crossing through improved detection of impostors. Biometrics included in the e-Passport can also be used to improve the quality of the background checking and detection of multiple applications performed as part of the passport application process.

An additional layer of security is added when the authenticity of the data on the e-Passport's chip is validated at the border using PKI certificates downloaded from the ICAO Public Key Directory.

While the deployment of an e-Passport program by ICAO Member States is not the subject of an ICAO standard, it has been designated as a recommended practice.

Recommended Practice 3.9 of Chicago Convention Annex 9:

[4] APEC GUIDE http://www.dhs.gov/xtrvlsec/programs/content_multi_image_0021.shtm

*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.*

## *3.2 Document Security Features*

The physical document, once personalized, does not remain under government control and is easily accessible to a large segment of the population. With widespread access to low cost technologies including high quality scanning, colour copy, image processing and photo quality print, the capacity of individuals to produce convincing counterfeit documents and very deceptive alterations has increased exponentially[5]. The passport can be subject to several counterfeit and alteration techniques, such as

- counterfeiting a complete travel document;
- photo-substitution;
- deletion/alteration of text in the visual or machine readable zone of the biographical data page;
- removal and substitution of entire page(s) or visas; and
- deletion of entries on visa pages and the observations page.

The passport must therefore incorporate security features to prevent easy alteration or deletion of the data it contains, or production of counterfeit documents or replication. A variety of security measures and techniques exist and the use of a good combination of these features is recommended to address different forms of potential attacks to the document. To be effective, the features should be easy to check and make a decision for officials who are required to examine the document. Three categories of security features are commonly used:

- Level 1 – can be examined unaided under normal lights conditions
- Level 2 – can be examined by simple hand-held tools (loop, UV light)
- Level 3 – require more specialized equipment to examine (forensic)

In order to ensure the physical security of documents and the information they contain, the document security must be updated on a regular basis. More advanced and secure technologies should be incorporated in each new versions of the passport. The features contained in the different versions of the passport must be communicated to all officials required to examine the document.

[5] Standard 1.1.3

Standard 3.7 of Chicago Convention Annex 9:

*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.*

The passport issuing authority should lead, and be the approval authority for, the design of the passport and selection of materials used in it. In addition the passport authority should be verifying that the materials being used to fabricate the passport are of a consistent and high quality in order to assure that the passport will not degrade in normal use, as well as to prevent counterfeiting and deter alteration. It therefore has a primary stake in working closely with the companies or government printer responsible for paper and consumables manufacturing and fabricating the passport and in making certain that at least some of the materials used are unique to the passport, or at least not available to the general public.

Off-the-shelf hardware may be used, but it is recommended that it be altered so that it produces one or more unique features in the document that are not available to the general public (for example, broken faced type); or that materials used with the equipment such as inks are uniquely designed so as to be readily identifiable as a product of that process only.

One of the most important travel document security feature of the last decade is the use of digitized photo passports. The use of such technology is the single most effective tool to impede photo substitution, which remains the number one abuse of travel documents[6].

All details on security measures to be applied to travel documents can be found in a technical report titled “Security Standards for Machine Readable Travel Documents” which was adopted as an Informative Annex of Document 9303 Volume 1 Section III. Since the publication the Informative Annex, new techniques and technologies have been made available to further improve the security of documents. This Annex is therefore being reviewed and updated by the NTWG/ISO to include most recent and state of the art document security features.

## *3.3 Validity period*

ICAO is recommending a validity period between five to ten years for regular passports. Because security features in a secure document can be compromised after only a few years of implementation, it is a good security practice to limit the validity period to five year. It enables withdrawing compromised books from circulation in a timely manner and introduction of redesigned and more secure versions of passports. However, service, volume and financial implications are important elements to be taken in consideration in the determination of the passport validity period. ICAO does not allow extensions to the validity of the passports.

Recommended Practice 3.16 of Chicago Convention Annex 9:

[6] WP 13, TAG 18 – UIMRTD Photos and printing.

*When issuing or reissuing 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.*

Standard 3.4 of Chicago Convention Annex 9

*Contracting States shall not extend the validity of their machine readable travel documents*

# 4 Personnel - Internal Fraud

To deliver its services to the population, the passport issuance organization is dependent and vulnerable to its staff actions and decisions. Thus it 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 making sure that staff to be employed is dependable and may not be easily corrupted. Once hired, employees may be subject to various external pressures to commit fraud and therefore special care must be taken to ensure the continued reliability and loyalty of individuals. Internal control to limit the authorities of employees, in addition to discourage and uncover staff malfeasance must also be in place.

Organizational structure, task routing and work environment, as well as internal policies and controls have a great influence in preventing and detecting internal fraud. If fraud is detected, an organizational framework needs also to be established to proceed with internal investigations and possible sanctions.

## *4.1 Hiring personnel*

Before employees are offered a job, there is a need for background and reliability checks. Contractors should also undergo these checks. The degree of the check should be related to the responsibilities, the access, and the level of decision-making that the employee will have. Nature and degree of the checks may also depend on some country's culture and tradition (examples?).

At a minimum, checks should be made against law enforcement databases. For those who perform management functions, and those who make the decision on entitlement to a passport, the checks should be more thorough and may include family, friends and previous employer interviews, as well as review of financial history. Security checks on employees should be redone regularly on a prescribed schedule during the period of employment. Although there is no mechanism to assess the potential of an existing employee for malfeasance, periodic background checks can highlight staff who are living beyond their means. 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.

Another threat to keep in mind is the possibility of putting “clean” employees (those with no criminal record or other cause for suspicion) on an issuing authority's staff. Such people will likely pass security clearances, and it is why internal controls and procedures that limit the access and authorities of employees are an important area of focus.

The security screening process should not allow a person into an area unless his/her duties require such access. Limiting the areas which personnel are authorized to access will reduce the opportunistic risk that these individuals will pose[7].

[7] RCMP Access control

## 4.2 Security training and awareness

Once a new employee reports for duty with the issuing authority he should be given an oral security indoctrination and written guidelines on the issuance authority’s internal controls and policies. Individuals must be briefed on their access privileges and prohibitions attached to their security clearance level. At the beginning of their employment, employees should also be introduced to the organizational standards of conduct or values and ethics guidelines. Time should be provided to the employee to read them and ask questions. Managers should ensure employees’ understanding of the standards of conduct.

In Chapter 1 - Passport Issuance Organization chapter, we touched on the importance of providing regular security training and information session to maintain employees security awareness. New employees and those on staff should routinely be addressed by managers and security personnel about security measures and policies, and what to do if an outsider or another employee approaches them to participate in a fraud scheme.

## 4.3 Morale

Greed is a motivator for employees to malfease. There is another motivation: anger at the way that an employee has been treated by the issuing authority.  Briefly put, an unhappy employee – one who (for instance) has been denied a promotion, or whose boss is a harsh taskmaster – is at greater risk of responding positively should they be approached to participate in malfeasance. Issuing authorities are well advised to pay attention to employee morale issues.

Job satisfaction is one of the most important factors in making employees loyal to the organization. Several elements influence morale and job satisfaction and include but are not limited to: fairness in pay, working conditions, free-conflict environment, good supervision and communication, involvement in decisions, training opportunities to qualify for higher graded work, good leave and other benefits of employment, etc. These are best managerial practices for any organizations but are even more important for organizations whose mandate and work may impact on national and international security.

Employees with high morale who feel valued for the contributions they make, feel loyalty to the organization, and are more productive and effective in their jobs. The most effective anti-malfeasance device available is to build a sense of self-respect and pride in the accomplishments of the organization. The working climate has to reflect that the employer really cares about people and their work. Employee recognition systems play a large part in this, and everything from (for example) organizational and public appreciation, awards or paid time off from work should be used to point out the plusses of an individual employee’s performance.

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

It cannot be overemphasized that the time and expense of training supervisors and managers to be subject matter experts and to develop the competencies of good management is a worthwhile investment that improves productivity and deters employees from participating in internal fraud.

## *4.4 Internal controls*

### 4.4.1 Organization

Every change in staff responsibilities, technology upgrades, requirements of the public, and operational methods and practices brings with it possible changes in the Internal Controls landscape. Thus, it is important to have a senior person designated at the Headquarters level, and at each production site, to make certain that internal controls considerations are factored into management decisions.

At the national (HQ) level, the designated Internal Controls Manager should be a senior officer who has ready access to, and is a participant in, the planning and decision-making levels of the organization; preferably someone not in the operations chain of command and who reports to the director of the issuing authority. The reason for independence from operations is that the primary responsibility of the operations office is to issue passports, 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 field (issuing) office level, a senior officer should be designated as the Site Internal Controls Officer (ICO). It is critical to have one person at the management level ultimately responsible; preferably someone who knows the work in detail. Naturally, successful administration of the site's internal controls program should be a critical element in that officer's performance evaluation.

There should be an Internal Controls Standards Handbook that puts in one place all the procedures that have been developed to minimize vulnerabilities, and emphasizes management's support of the internal controls program; and the responsibilities of all individuals with regard to the security of assets.

The site ICOs should have a checklist of internal controls procedures for which they are responsible, and should be required to use it in between HQ on-site reviews to do periodic full local reviews of IC compliance.

The position descriptions of all staff should have an internal controls standard of performance included that imposes a requirement to be aware of and adhere to internal controls. And ratings of all staff should include evaluation of internal controls performance. Disciplinary measures for neglecting one’s duties and responsibilities should be described at employee orientations and assessed as part of performance reviews.

## Routing of Work

Prescribed job functions should be established such that one employee cannot perform all the passport approval and/or issuance functions. This means that it will require a conspiracy involving two or more employees to issue a passport to someone who has tried to buy one through subversion. It has been proven that it is harder to arrange a conspiracy to commit malfeasance than for one person to do so, and it is far more likely the issuance authority will uncover conspiracies than lone malfeasants.

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 passport 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 “his” line). The same principle applies with desk adjudication. Staff members should be required to take the next batch of work in sequence. This reduces the possibility of staff members being able to access specific passport applications-in-process. For the same reason, staff members should be required to rotate through all adjudicative functions (dealing with the public, desk adjudication of mailed applications, handling submissions of better citizenship evidence, and dealing with VIP applications, and others).

Staff must not approve passport applications of friends and family, or bring them to work and insert them into the issuance system without a supervisory signoff. If an employee brings in an application for processing, it should be given to the supervisor of the entitlement staff for approval. Similarly, applications of VIPs and others accepted by managers should be given to the supervisor of the entitlement staff for approval before passport issuance.

It should be required that adequate notations regarding evidence seen and actions taken be present to justify the actions directed by entitlement (adjudication) staff, both to provide adequate written justification for passport issuing staff to take the requested action, and so that actions taken on the application may be reviewed later in 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.

It may be necessary that applications accompanied by specific types of less reliable citizenship/identity evidence must be routinely referred to the fraud unit for review and document checks. Prescribed minimums should be given to all examiners.

Some applications that are especially difficult should be reserved for final approval by more senior entitlement staff, including complicated citizenship cases, replacements for multiple lost and stolen passports, reissuing a passport because the first one has not come in the mail, cases in which applications have been found deficient and the applicant has submitted additional evidence, and others.

### Automated systems

Leveraging technology to automate passport issuance processes can increase the security of passport issuance process and enhance accuracy. Data entry, scanning, printing, archiving, mailing and management reporting processes can all be automated to a certain degree. This limits the involvement of manual manipulation of data, and may improve the rapidity of detection of fraudulent or questionable information.

### Protection of personal information

The passport application forms contain some personal information. This information is protected by privacy laws, and should not be disclosed to third parties. Staff of passport issuing organization should receive training and documentation on the various information and privacy laws effective in their countries, and management must enforce these laws. In addition to privacy concerns, communication of this information to outside parties can lead to identity frauds.

### Treatment of VIPs

To complete

### 4.4.2 Audit trails

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

Formal internal audits and compliance reviews should be done by senior officers from the issuing authority’s headquarters to review operation management and the adequacy of the internal security division’s controls program. A formal report of findings should be produced by the inspection team, and their recommendations for improvements should be sent to the agency head by the issuing authority director.  Headquarters should then have a compliance process that assures that needed changes are implemented.

An external and independent organization such as the governmental audit office should also perform regular performance audits to evaluate the passport issuance agency's security good practices. These independent organizations usually produce some recommendations and are monitoring their implementation.

These formal audits should be supplemented with active review of work in progress by managers who understand the work processes, and randomly check them to make certain that established rules are being complied with. This is true at all times but especially in periods of high workload when staff and management may be tempted to cut corners and ignore some internal controls. Internal reviews should utilize senior officers in local offices to look at a percentage of the most urgent applications, other applications in process, and issued applications, verifying that proper procedures have been followed, that evidence attached or recorded is adequate, that notations are complete and justify the actions directed, and that proper fees have been paid.

## *4.5 Internal investigations and sanctions*

Allegations of possible malfeasance may arise from within the issuing authority, or from outside. In fact, employees should be encouraged to advise management when they are approached by persons wanting them to commit fraud, and if they become aware that another staff member is involved in fraud. There should be an established process for handling such reports and for referring them to the appropriate investigating agency or section separate from operations.

It should be clear what agency of government has responsibility for investigating passport fraud. Often the responsibility will be split, with one agency having responsibility for external fraud and a different agency handling internal fraud. But whether one or two, it is important for the issuing authority director to meet with the leadership of the agency(ies) responsible for fraud investigations, both to be informed about cases in process, and to make certain that the issuance authority is cooperating fully.

The findings of internal fraud investigators should be conveyed fully to the issuing authority, especially in the area of what was done and how. This is important because the issuing authority needs to learn whatever lessons there are from every instance of internal fraud, and should take rapid corrective action to prevent a reoccurrence. Through effective reporting and investigation of security incidents, vulnerabilities can be determined and the risk of future occurrence reduced.

Make certain that there are adequate laws to bring charges and prosecute employees suspected of internal fraud, and that the law provides for meaningful penalties. Sanctions should be given in response to security incidents when there has been misconduct or negligence.

Persons determined to be responsible for committing internal fraud by investigators should normally be released for cause. This applies to those who have "only" done something small.  They have shown a willingness to break the rules, and if not honest on small matters may not be trusted on larger matters.  In addition, if warranted, they should be prosecuted to the fullest extent of the law.  At a minimum, their security clearance should be revoked, suspended or downgraded.

The issuing authority should press for significant penalties not only for the punishment involved, but even more importantly, as a deterrent -- proof to other employees that involvement in internal fraud is risky and that there are real penalties. Publicize the results of every case (conviction, dismissal, or resignation).  Don't leave it to chance that the other employees will somehow hear about the findings and punishment.  Those who felt betrayed by their former colleague need to know that the person was punished.

# 5 Physical Security

Buildings and offices where the passports production and issuance are taking place must be secure to address unauthorized access by external or internal individuals. This touches both facilities and processing systems.

Physical security is also to ensure the health and safety of employees at work. There may be situations where employees are under threat of violence because of their duties or because of situations to which they are exposed.

## *5.1 Access control [8]and monitoring*

Control of access is an important component of a physical security approach. Of course, the effectiveness of controlling access depends on the nature of the threat. Access control will provide minimal protection from those who have already access to the facilities (internal fraud). Monitoring equipment will be useful to survey some zones that necessitate higher security.

The access to passport production offices must be controlled and limited to those who have undergone a screening process to the appropriate security level. At times, visitors or contractors may have duties in an area but not have undergone the appropriate security screening. They should be escorted at all times. Cleaning staff and security guards must also be security cleared.

Passport offices and production facilities can be divided in different zones to which different means of access control should be adapted.

- public zone (i.e. surrounds the facilities) - no access control.
- reception zone (i.e. initial contact between visitors and organization) - access may be limited to specific time of day.
- operations zone (i.e. office space) - access controlled.
- security zone and high-security zone (i.e. passport production, blank handling areas, cash handling areas) - access controlled, monitored 24/7, may include special security specifications.

Operations, security and high-security zones should be designated as “restricted” and access should be for authorized personnel only and not all employees. These include a vault area where blank passports are stored, the book production area where blank passports are personalized, and the cashiers area, where cash is handled and accounting for money takes place.

[8] Physical Security Guide G1-024 RCMP

There are a variety of methods to control access and monitoring, each of them providing different levels of protection (at different costs). A combination of strategies should be used. Considerations should be given to the level of inconvenience that each option provides. The control of access should be as convenient to normal operations as possible. Find below some strategies that could be employed in all facility processing passports:

- Security personnel who have the task of providing on site security for the building 24-hours-a-day, seven days a week.
- Access badges, to be worn at all times by employees while in restricted zones. If employment is terminated, the access badge must be recuperated by the organization. Visitors and contractors should have temporary badges in exchange of acceptable photo identification. Staff members are to sign in visitors and the identification will only be returned once the visitor access badge is returned.
- Electronic or physical barriers at entry points (i.e. doors, turnstiles, gates)
- Locks using limited distribution keys, pin numbers, electronic cards or keys, or biometrics. Pin numbers should be changed on a regular basis.
- Intrusion detection:  alarms, motion sensors
- Surveillance: doors monitors, cameras, CCTV
- Movement of material should also be screened in an appropriately located mailroom. Mailroom staff should be trained to screen for suspicious material and initiate a protocol once a suspicious package has been identified.

Even during working hours, the exterior doors should remain locked, with only government employees (not contract staff) having keys and combinations.  Others needing entry should be monitored and admitted using visual-recognition door monitors and a remote door-release mechanism.

It is recommended that, outside of normal working hours, pending work be locked up so that building guards, issuing authority employees, or cleaning staff will not have access to private information of applicants that is not needed to perform assigned tasks.

### *5.1.1* Customer Service area

The area where the public comes to apply for and receive passports should be built so that customers cannot have easy physical access to staff (for the safety of the staff and the security of the passport-making materials), or to the passport fees that are being paid. Physical security may include duress alarms, glass or other screening, and magnetometers to detect weapons carried by applicants (if that is a concern).

It is also recommended that security personnel be present during working hours to provide a calming presence if applicants become agitated, and to escort applicants out of the area should they become disruptive.

Finally, there may be a secure interview room where law enforcement agents can interview possible fraud perpetrators who are caught when applying, or when they come back to pick up a passport. It may, however be preferable in certain circumstances for law enforcement personnel to remove the person for questioning.

## 5.2 IT Security

In the past we were able to protect information by simply controlling the physical access to that information. In our modern networked age this is more of a challenge - vast quantities of the information in our safekeeping is on interconnected networks of computer systems. Passport issuance systems are not an exception. They are more and more automated and are using information technology to improve service delivery. Online passport applications are also being introduced in many countries. At the same time, the number and potential severity of threats, vulnerabilities and incidents similarly increase. Because passport-issuing agencies demand the collection of a lot of personal information, sometimes including biometrics, the protection of IT systems and databases is crucial.

IT security is defined as the safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information. Without going into details, vulnerability assessments on the various IT systems and processes should be performed regularly to implement protection measures. 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.

Access to passport issuance system must be restricted. The equipment should be limited by means of passwords that allow an authorized employee to log on to the system, and access codes in the central system that give an employee permission to perform specific tasks. Passwords should be random number and letter combinations that can’t be guessed (birthdays, parent’s names, etc.).

The equipment should have access controls that prevent its use except by authorized staff and indicate who has had access. Computer records of logon usage should be maintained for a reasonable time, and logons should be forced by the system to be changed regularly. Access logs of computer activity should be generated for review by management personnel to identify irregularities in computer access.

The organization must inform and regularly remind personnel of their IT security responsibilities, concerns and issues and provide training. In case of an IT security incident, investigation should be performed and sanctions given if it is found that there has been misconduct or negligence.

# 6 Treatment of Blank Passports

Blank passports include passport blank book, identification and observation labels as well as security laminates. The protection and secure management of blank passports and raw material is critical to the integrity of the passport production program. Blank passports and material that are lost or stolen can be used to create very persuasive counterfeit documents, and it is therefore a critical threat for the integrity of passports.

## *6.1 Numbering*

Passport blanks should be produced using a sequential numbering system so that individual documents are uniquely numbered to facilitate accountability as the passports are made and in shipping to the passport issuance authority; and later on in the issuance process. In some cases this number may become the passport number. In other cases where that is not the case, the passport accounting records should be retained for at minimum the period of validity of the passport.

## *6.2 Storage*

Blank books should be contained in approved secure repository, with access limited to those who have supervisory authority over production staff. Access to blank book storage should be limited to the smallest number of persons possible. Assigning blank books to production staff should be conducted by at least two employees (4 eyes principle, dual signing).

## *6.3 Accounting*

The inventory control numbers put into the passport blanks when produced should be tracked from the time the passport blanks are shipped by the manufacturer, and should continue to be tracked until each and every one is accounted for as a completed passport or a spoiled book. The tracking records should be maintained throughout the validity period of the passport.

This involves counting and recording blank passport totals every time they change hands, and a default process for handling spoiled and defective books, such that if they are to be destroyed, there is an accountability process that matches back to the master inventory.

The actual destruction of spoiled, defective and excess blank or partially completed passports should be conducted and witnessed by two responsible staff members.

Blank passports should be counted out of the locked repository in the morning, and unused passports should be counted back in, employee-by-employee, each night by two individuals. The actual count of blank passports should be reconciled daily at the end of the day to make certain that the count of passports on hand matches what the automated inventory says should be on hand. If the latter record is maintained by hand, reconciliation is still required.  Records should be maintained for at least the validity period of the passport.

# 7 Application and entitlement Decision

Because of the technical developments mentioned earlier, there has been a displacement of fraud. People who committed fraud used to stand at the end of the chain, where they occupied themselves with the forging or falsification of travel documents; now they stand at the beginning of the chain[9]. While a lot has been done to enhance security of the passport, security efforts must focus on the weaker parts in the issuing process. The primary or breeder documents, used by the passport issuing authority to determine identity and citizenship, are usually issued by various local or regional authorities. They often contain less security features and are not standardized. Security efforts must focus of how the passport entitlement officers are analysing and using these documents and how they are equipped to detect frauds.

## *7.1 Verification of identity and citizenship*

### Breeder/primary documents

Confirmation of the identity of passport applicants is the key to passport integrity. The issuing authority must be certain of the genuine identity of the passport applicant. The only way to be certain is for the passport applicant to identify him- or herself using a document or combination of documents that gives reasonable assurance to a trusted representative of the issuing authority.

In most countries there are two necessary elements that a government needs to establish before issuing a passport: evidence of the applicant's identity, and proof of citizenship. Documentary evidence to establish entitlement under both these requirements is often combined in a single card. It has to be a good quality document, issued under the supervision of the national government, and it contains a biometric or clear photograph. Without those features, the passport issuance authority may still be vulnerable to persons stealing the card/identity of another person (living or dead).

In many countries, the two types of records described above (called "Breeder" or "Primary" Documents because they are used to obtain higher level documents) are issued, stored and retrieved separately and are often issued by local or regional authorities with little or no national standardization. Persons who would obtain passports in false identities can use many methods to obtain breeder documents, from theft to taking advantage of loose application procedures, to creation of false identities based on deceased individuals, to counterfeiting reasonable facsimiles, filling them in and presenting them as genuine.

[9] Ronald Belser - 9303 part 4

Applicants must turn in their documentary evidence with their application so that it can be verified by unannounced audit at any time during the adjudication and issuance process. It is then returned to the applicant with the issued passport.

Staff accepting passport applications and adjudicating entitlement to passports should be trained in both the characteristics of genuine breeder documents and the identification of false documents. The document, often a birth certificate, probably also exists in many different forms. It is said that the United States of America has more than 7,000 different types of birth certificates in circulation. This complicates the identification process related to the issuance of travel documents.

Ideally, the issuing authority's own trained staff will perform verification, but the larger the country and the more application locations there are, the more likely it will be that the issuing authority will have to partner with other organizations that are well represented locally. It is recommended that a country with this need partner with governmental institutions that are familiar with legal process and paperwork, such as courts, police, post offices, or other government offices that are used to dealing with the public, such as tax offices or government operated libraries. Partners of the passport authority should also be trained to perform verification of breeder documents. In case of doubts, cases should be referred to the passport issuing organization.

ADD - Evidence of identity

## In-person application

Many countries require personal appearance for every new passport, including renewals, but it is arguable whether that is necessary. Adults who can be properly identified by matching their old passport with new photographs need not appear in person. However if the previous passport is in a false identity automatic renewal perpetuates the problem. On-line verification with primary source document agencies (e.g. birth or citizenship records) is recommended. This will help to confirm legitimate documents and rapidly identify fraudulent ones. These might include local registrations of birth and death (preferably in a national/virtual database, with births and deaths linked), retirement programs, health insurance, driving licenses, census records, and family status records.

Those applying for a passport for the first time, children under the age of majority, and persons who cannot present their most recent prior passport should appear in person to apply for a new passport.

Passport application acceptance agents must be trained in how to do this work, and should have detailed written guidance on how to identify passport applicants, how to note the identifying documents on the passport application, and what to do in the event that they are not satisfied with the identity documents presented. Staff should be trained in other skills that will help to highlight other signs or indicators of a fraudulent application, for instance:

interviewing skills, body language recognition skills, and the ability to see inconsistencies in the totality of the applicant's presentation and documents.

## Guarantor and references

An alternative to interviews that has been successfully utilized in many countries is a process of designating professionals such as doctors, lawyers, clergy, etc. to countersign passport applications attesting to the identity of the passport 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-signatory should be those that maintain records of membership through a recognized association. But it has the problem of being difficult for the issuing authority to keep track of all the people authorized to countersign, and it is virtually impossible to train such a large and geographically spread-out group. On balance it is believed that a required appearance before some sort of governmental official offers a better chance of identity confirmation for the wide range of applicants. This is especially so for countries which have a highly transient or mobile population, where people move frequently for work, and consequently do not become well known in their community. This also reduces the chance of fraud committed as a favor to people with whom there is a close personal or financial relationship. The use of one or the other means of identifying individuals, by personal appearance or a counter-signatory, improves confirmation of identity and is recommended.

As a last resort, persons who have not been able to identify themselves adequately by documents, may ask people, especially family, who have long and/or personal knowledge of the applicant to witness to their identity in written form, under oath or penalty of perjury. The affidavit of identity that is executed as part of this process should be completed by a passport holder if possible and should become a permanent part of the passport application file.

## Anti-fraud unit

It is recommended that issuing authorities create an organizational entity at the Headquarters level with a primary focus on fraud prevention; with the tasks of coordinating field anti-fraud operations, providing training resources, providing back-up on difficult casework, and liaison with other entities of government that produce breeder documents (toward improving them), and those that prosecute fraud when it is found.

At least one representative of this Headquarters office should be assigned to every passport issuing office as a fraud specialist and fraud prevention manager. That officer (or staff in larger field offices) would have the tasks of training and retraining appropriate staff in fraud recognition skills, the researching and resolution of suspect cases referred from front-line staff, analysis of casework and contributing to national fraud trend reporting, and local liaison with law enforcement.

## *7.2 Verification of travel restrictions*

The name, date and place of birth of each applicant should be checked against an electronic data base containing the names of persons who are not entitled to a passport for various reasons; for example, persons who have been involved in passport fraud in the past, persons wanted by law enforcement for criminal activity, for failure to pay child support, etc.

The system should be designed so that hits will be of two types: matches, and trials. The latter occur because something in the database (common names, for instance) is a close match to the entry. The name clearance process should be early enough in the application handling process so that a passport will not be issued and released prior to clearance being given. Also, resolution of the hit (including voiding of trial hits) 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 hit, and some percentage of those overrides should be reviewed by supervisory staff.

The parameters of electronic name clearance systems need to be set so that hits will occur with close matches rather than exact matches. For instance, with the use of names, applicants will sometimes provide a middle name, a 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, and since the clearance process often takes place before entitlement adjudication, hits may be missed if the parameters are set too close. For this reason it is also wise to clear again the names of those applicants whose data elements are changed in the adjudication process. It is also recommended to clear former names when names have been changed by court order, marriage, etc.

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

## *7.3 Use of biometrics*

TO COMPLETE [FR, Fingerprints]– Use of FR to compare photos submitted with the application against a database of previously issued passports to confirm that a passport has not already been issued to the applicant under another name; and a database watch list of ineligible applicants.

In developing a biometric enrolment process, it is important to keep in mind that there should be adequate safeguards to assure that the identity of the enrolee is properly established and thoroughly documented.

## 8 Delivery of personalized passports

A passport may be released to the applicant in person, sent to the applicant by mail or courier services, or released to a third party if a written authorization is provided.

Having the applicant pick up their own newly issued passport is suggested, though a high volume of applicants coming into the office may be a problem. When releasing the passport, the employee should compare and verify the photo in the passport to the photo in the system and the applicant. If released to a third party, a written authorization should be provided and the identity of the person should be established using identity documents. A receipt should be signed by the person picking up the passport.

Using reliable mail services to deliver the passport is an alternative. Is your mail service reliable? If not, use controlled mail if necessary to reduce the possibility of theft of issued passports from the mail. If mail service is unreliable, consider using reliable private delivery services [courier services].

The fact that a passport that comes back to the issuing authority undeliverable may be a fraud indicator, and it should be checked against the application. If the address is correct, the applicant should be contacted to come in and pick up the passport. Otherwise the file should be referred to fraud investigators. Passports reported as undelivered should be handled as lost/stolen passports. They should be immediately declared invalid, and put into a lost/stolen passports database.

## 9 Lost and stolen passports[10]

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

Misuse of genuine documents obtained in unlawful circumstances creates serious national security and public safety issues that must be addressed within each national authority. 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.

### *9.1 Public communication*

Encouraging citizens to take care and keep their passport safely at all time is important. This will help to protect the passport against being stolen. Once issuing the passport, the public should be informed on what action to take should the document be lost or stolen. Such guidance should also highlight that once a passport is reported lost/stolen; it will be cancelled and is no longer valid for travel. The public should be required to report lost, stolen or missing passports to the police and to passport issuing authorities as soon as the loss is discovered. It should be clear how document losses and thefts should be reported and make it easy to report the incident in person or by phone, mail, fax or e-mail. A public awareness campaign to sensitize passport holders to this is recommended.

Encouragement through public awareness campaigns is helpful. Also helpful is the expectation by citizens that obtaining a replacement will be difficult or expensive.

Requests to issue replacements for lost and stolen passports represent a vulnerability and should be screened carefully by adjudication/entitlement staff for indications of fraud. Replacement passports should be limited in validity if there is a history of previous lost passports. Other possible deterrents include higher fees for replacements, a mandatory endorsement identifying the passport as a replacement (which will tend to draw the attention of immigration officers), mandatory hold time between application and issuance to permit investigation, and refusal to issue another passport after (for example) a second lost passport, or where evidence has been obtained that a reported stolen passport was actually sold or loaned.

### *9.2 National lost and stolen passport database*

[10] G8 Best practice for the processing of travellers who present lost of stolen travel documents

Lost and stolen passports should be declared invalid, and should be immediately listed in a lost and stolen passport database. These databases provide the means to analyse and risk assess the individual national situation in relation to travel document security. The database should hold information specific to the circumstances of the individual or collective loss of these documents. It is recommended that each government ensures such a database is maintained and that it can be accessed as part as the border crossing process. Once declared lost or stolen, these passports should not be returned to circulation.

## *9.3 Information sharing*

There has been long–term acceptance that the global interchange of information on lost and stolen passports is a key risk mitigation strategy in relation to border control and identity theft. This enables the States to identify the use of their own lost and stolen passport, but also the documents issued by other States.

It is recommended that data relating to all lost, stolen or cancelled passports or other travel documents be reported to Interpol as soon as possible. Access by border control authorities to the Interpol Lost and Stolen Database, which was created to provide information on lost and stolen travel documents to the international law enforcement community, would greatly increase their ability to intercept travellers presenting lost, stolen or cancelled travel documents. National databases can assist with the ready transfer of the required information to Interpol Lost and Stolen Database to ensure that if used, the document can be intercepted and any potential criminal activity prevented. The Interpol Lost and Stolen Database system requires minimum data consisting of a) Document number, b) Issue data, c) Type of document and d) Nationality of document.

The G8 Roma-Lyon MESG has developed a document titled 'G8 Best Practices on Quality Control of Reporting on Lost and Stolen Travel Document Data' that can guide the reporting of lost and stolen passports to Interpol.

# 10 National and International Stakeholders

## *10.1 Border and Immigration Agencies*

- Importance of collaboration with border and immigration agencies
- Data sharing

## *10.2 International Partnership*

Many international working groups are involved in the development of standards and best practices related to the issuance of passports and other related subjects. These groups are information exchange clearinghouses and offer the opportunity to learn from the experiences of others.

Standards - interoperability

Data sharing

Capacity building available

# PART 2: ASSESSMENT GUIDE

- Checklist
- Evaluation scale to globally evaluate the performance of the organization regarding security of the issuance process

The following checklist is provided as a guide to assure that relevant security considerations are identified in developing or reviewing the passport issuance process of relevant organizations.

**Passport Issuing Organization**

- □ Who manufactures your blank passports?
- □ Please describe your organizational structure as to dispersion of offices, personalization, and related regarding centralized and decentralized structure.
- □ How do you anticipate workload shifts and adjust for them?
- □ What are the procedures for adjusting your fees?
- □ Do you keep all or any portion of your fees?
- □ Are the passports used as identity documents for other purposes than travel, such as at banks?

**Overseas Delivery**

- □ Do you issue passports at overseas missions?
- □ If so, do you have written requirements for the delivery and storage of blank passports overseas? Please provide any such statements.

**Document Security**

- □ Does your state currently issue machine readable passports (MRPs)?
- □ Does your state currently issue e-Passports?
- □ Have you used the ICAO 9303 standards to design your passport?
- □ Is your passport in compliance with 9303 standards, in particular those relating to security – Informative Appendixes 1, 2 & 3 to Section III?

**Document Security Features**

- □ Does your document employ a number of different types of security features?
- □ Have you done testing to determine such things as the durability of your passport materials?
- □ What is the split between 1st, 2nd and 3rd line features?
- □ When was the last time you redesigned your passport?
- □ Does your passport have a digitized photo?
- □ What personalization technology are you using? ex. Ink jet D2T2, etc
- □ What security laminate do you use?
- □ How much lead time does your printer require?
- □ What is the validity of your passports?
- □ Do you allow extensions to the validity of the passport?

**Physical Security**

- □ What kinds of security measures do you use to control access to your facilities?

- ❑ Once access has been granted, what kinds of measures do you employ to insure that only those employees who have a work-need to enter an area, e.g., blank passport storage vault, are able to enter?

**Personnel**

- ❑ Throughout your issuance processes, do you have divisions of labor among your staff that guarantee that no single individual can issue a passport?
- ❑ As an application proceeds through the steps, do you have measures in place to control each step and insure that only those individuals authorized to engage in those processes are able to do so?
- ❑ Do you allow staff to process applications of family members?
- ❑ Can you trace back after a passport has been issued and know exactly those staff members who were associated with processing the application?
- ❑ Do you conduct security checks on your staff before hiring them?
- ❑ Have you found it necessary to discipline staff for work related problems, especially, but not limited to, security breaches?
- ❑ What are the penalties?
- ❑ Do you conduct assessments of vulnerabilities in your program, especially with regard to your staff, but not limited to that area?
- ❑ Is your staff specifically trained in document abuse and counterfeiting and other aspects of fraud?
- ❑ If so, at what intervals is this training updated?

**Treatment of Blank Passports**

- ❑ Do you have written requirements about the ordering of book materials by your printer?
- ❑ Do you have written security requirements about the storage of these materials at the printer?
- ❑ Do you have written security requirements regarding the storage of blank printed passport books before they are delivered to you?
- ❑ Do you have written requirements to control the security of delivery of blank passports?
- ❑ Do you have written requirements to control the storage of blank passports at your facilities?
- ❑ How do you account for each book that is in process, that which is issued as well as those that are spoiled?

**Application and Entitlement Decision**

- ❑ Do you use birth certificates as part of your entitlement determination process?
- ❑ What kinds of checks do you make to insure that the birth record is genuine and rightfully belongs to the applicant?
- ❑ What other forms of documentation do you require in adjudicating applications?
- ❑ What kinds of validation checking do you do for each?
- ❑ Do you have access to civil registry databases such as birth, death, tax and other records?

- □ Do you use live photo capture, photos submitted by the applicant or both?
- □ Are you using the ICAO photo image quality standards for your photographs?
- □ Do you use biometrics as part of the issue procedures?
- □ Do you use other biometric indices such as fingerprint or iris?
- □ Do your procedures for renewals differ from the original application?
- □ Do you adhere to the one-person-one-passport, regardless of age, best practice of ICAO?
- □ Do you read the machine readable zone (quality assessment) of each passport before giving it to the applicant?

**Lost and Stolen Passports**

- □ Do you contribute to the Interpol lost and stolen travel documents database?
- □ What kinds of uses do you make of lost and stolen data?

**Reading passports**

- □ Is your country reading the passports at border inspection?
- □ Are any other users of passports as identity documents, such as banks, equipped to read the documents?

# ANNEX 1 - REFERENCE DOCUMENTATION

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

## ANNEX 2 – ABBREVIATIONS

— END —