For Publication on the ICAO Website

Guide for Assessing Security of Handling and Issuance of Travel Documents

Part 3- A Guide for Experts

DISCLAIMER: All reasonable precautions have been taken by the International Civil Aviation Organization to verify the information contained in this publication.
However, the published material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader. In no event shall the International Civil Aviation Organization be liable for damages arising from its use.
This publication contains the collective views of an international group of experts and does not necessarily represent the decision or the policies of the International Civil Aviation Organization.

Version: Release 1

May 2016

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

Guide for Assessing Security of Handling and Issuance of Travel Documents

Part 3 - A Guide for Experts

May 2016

Table of Contents

Introduction

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

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

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

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

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

Consider:

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

Current Situation:

Strengths:

Weaknesses:

Recommendations:	C/N

C= critical N=non-critical

Chapter 2 – Application Process

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

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

Consider:

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

Current Situation:

Strengths:

Weaknesses:

Recommendations:	C/N

C= critical N=non-critical

Chapter 3 –Entitlement Process

Why is this important

To ensure document integrity three elements need to established as part of the entitlement process: evidence of the applicant's identity, i.e. this is a real identity and the applicant is in fact the claimed individual; proof of citizenship; and, verifying if the applicant is subject to any travel restrictions, e.g. criminal record, history of lost and stolen travel documents, failure to pay child support, etc. It is critical that establishing identity is carried out to the highest standard to prevent national travel documents being issued to those not entitled to hold them – this includes criminals and terrorists.

Consider:

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

Current Situation:

Strengths:

Weaknesses:

Recommendations:	C/N

C= critical N=non-critical

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

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

Consider:

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

Current Situation:

Strengths:

Weaknesses:

Recommendations:	C/N

C= critical N=non-critical

Chapter 5 – Personalization and Delivery

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

Consider:

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

Current Situation:

Strengths:

Weaknesses:

Recommendations:	C/N

C= critical N=non-critical

Chapter 6 – Document Security

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

Consider:

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

(Reference – Part 1 Chapter 6)

Current Situation:

Strengths:

Weaknesses:

Recommendations:	C/N

C= critical N=non-critical

Chapter 7 – Facility Security

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

Consider:

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

Current Situation:

Strengths:

Weaknesses:

Recommendations:	C/N

C= critical N=non-critical

Chapter 8 – Information Technology Security

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

Consider:

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

(Reference – Part 1 Chapter 8)

Current Situation:

Strengths:

Weaknesses:

Recommendations:	C/N

C= critical N=non-critical

Chapter 9 – Protecting and Promoting Personnel and Agency Integrity

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

Staff morale, work organization and internal controls have a great impact on the prevention and detection of internal fraud. Suspected or detected fraud needs to be investigated and possible sanctions must be in place.

Consider:

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

Current Situation:

Strengths:

Weaknesses:

Recommendations:	C/N

C= critical N=non-critical

Chapter 10 – Lost and Stolen Travel Documents

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

Consider:

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

Current Situation:

Strengths:

Weaknesses:

Recommendations:	C/N

C= critical N=non-critical

Chapter 11 – Overseas Issuance

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

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

Consider:

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

Current Situation:

Strengths:

Weaknesses:

Recommendations:	C/N

C= critical N=non-critical

Chapter 12 – National and International Stakeholders

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

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

Current Situation:

Strengths:

Weaknesses:

Recommendations:	C/N

C= critical N=non-critical