International Civil Aviation Organization

Sixth Symposium and Exhibition on ICAO MRTDs, Biometrics and Security Standards

ICAO Headquarters, Montréal, Canada
1 - 4 November 2010

Ensuring the secure environment in the passport issuance process: physical security and electronic security

Steven G. Grant, P.Eng.

Business Development Manager

Security Systems Division

3M Canada

Food for Thought

- The integrity of passports and other travel documents is a key component of national and international anti-crime and anti-terrorism strategies. (e.g. UN SC resolution 1373 obligations)

- Prevention of fraud is undeniably more efficient and much less costly than dealing with the consequences of successful fraud.

Recommended best practice:

- The passport issuing process should be recognized as having an impact on national and international security and be included in the governmental security framework.

Need for Passport Issuance Security Standards

- It is very likely that your passport issuance system will be attacked

- Successful attacks threaten social security & have potential for increased criminal activity

- Successful attacks put at risk the international reputation of your passport & its utility to citizens as a travel document

- A respected travel document facilitates travel and economic activity

Best Practices on Secure Issuance of Travel Documents

- Applicable to all ID documents including passports, visas, national ID, etc.

- Recommended Practices include:
    - Organizational and Personnel issues
    - Application, Entitlement and Delivery
    - Handling of Materials
    - Document Security
    - Physical Security and Information Technology Security
    - International (SLTD, Consular, Partners)

Organizational Structure

- Mandate, Responsibilities and Legislation

- Security Framework

- General Security Practices

Sixth Symposium and Exhibition on ICAO MRTDs,
Biometrics and Security Standards, 1 to 4 November
2010, Montréal
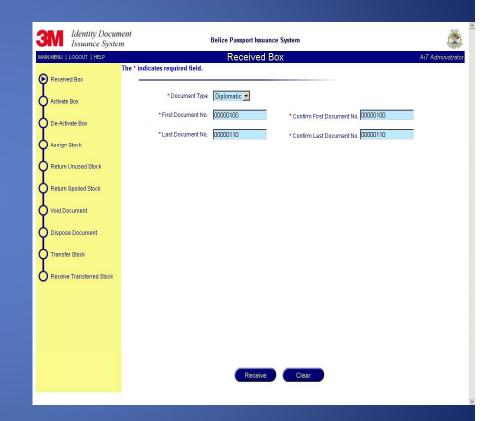
5

Treatment of Materials and Blank Books

- Book production

- Numbering

- Shipping and Storage

- Accounting
  - Inventory control, daily reconciliation, etc.

- Destruction

Example of Inventory Control

- From shipment arrival to issuance to applicant
- Document cannot be personalized unless
    - Stock activated
    - Assigned to site & operator
- Operator can only personalize documents assigned to them
- Spoiled documents recorded
- Stock reconciled each day
- Destruction of stock witnessed and recorded

Passport Personalization

- Printing equipment should include the capability of producing unique features
  - ability to identify a passport personalized on the system
- Physical security of equipment
- Passwords and secure access for operation
- Tracking who approved and performed steps
  - Audit Trail; periodic/random audits; work sampling

Physical Security

- Physical security of the passport issuing plant

  - controlled buildings/space

  - Presence of security personnel, alarms, TV, surveillance

  - Special requirements for vault & document personalization room

  - Applicants and security

  - Protection of applications in process (privacy)

Sixth Symposium and Exhibition on ICAO MRTDs,
Biometrics and Security Standards, 1 to 4 November
2010, Montréal

9

System Integrity and Security

- Network

- Access control

- Workstations

- Database and database operations
  - e.g. watchlist management

- Reports: production, inventory, audit

- Processes:
  - e.g. supervisor oversight, no single operator

Summary: Best Practices

- *The passport issuing process should be recognized as having an impact on national and international security and be included in the governmental security framework.*

- *The passport issuing authority should have clear mandate and responsibilities, established by legislation or suitably enforced regulations.*

- *Written security policies and guidelines should be developed and communicated to all. They should be strictly enforced.*

- *Independent from passport operations, a security team responsible for managing the security framework, should be in place.*

Questions?

Steve Grant

3M Security Systems Division

Tel +1 613 722 2070

Fax +1 613 722 2063

sggrant@mmm.com