Annex - Proposed Report to Information Commissioner's Office. To be submitted as letters to affected individuals are posted

Formal Notice of Data Breach
Investigation of 21 Lost Passport Applications

Summary of Incident & Investigation:

- 21 application forms for the renewal of a passport, along with photos of the applicant and the accompanying old passport to be replaced, appear to be lost from our Peterborough Regional Office. 14 were adult renewals and 7 were child renewals.

- The total number of people affected by this incident is **35**, including the parents and countersignatories of the child applicants, who also would have had some details included on the application form.

- The information that was included in these applications is as follows:
    - Name
    - Address
    - Gender
    - Date of Birth
    - Place of Birth
    - Signature
    - Contact telephone number
    - Parents name, date of birth, nationality, passport number (for child renewals)
    - Countersignatory name, date of birth and passport number (for child renewals)
    - 2 photos of the individual
    - Their old passport submitted for cancellation. Of the 21 passports involved, all but 7 were already expired whilst the others had no more than a few months remaining validity.

- They appear to have gone in small batches of 3 – 5 applications, with the exception of the latest batch which is a box of 10 applications. However, we have established that there is no evident link between the applicants or applications involved.

- The losses were detected when the box of applications in which they were held was passed into our application examination teams from the "file holding" room, where application forms are held after they are initially scanned into our system by Steria (our outsourcing partner) when received in the post. Applications are counted into file holding when received from Steria and all have been recorded as received in file holding.

- Actions taken so far to recover the applications and mitigate risk:
    - Full briefing of IPS and Steria staff, including re-iteration of key security processes.
    - Thorough search of the office by local and national IPS teams.
    - Thorough search of confidential waste bins on discovery.
    - Old passports cancelled and placed on stopfiles and lost/stolen lists (which are used at borders and by the Passport Validation Service.).
    - Notifications to CIFAS, SOCA and Interpol.

  - Review of access logs to file holding, especially focussed on identifying unusual activity
  - Review of box tracking information on our PASS system to identify any unusual activity.
  - Exercise by IPS central security investigation team to interview staff in Peterborough as a result of the access control/box log review.
  - Regular review of access permissions to File Holding brought forward. A number of people were removed due to changing job roles or a need to access the room on an infrequent basis – although none of those individuals have been involved in this incident.

- Following these actions, there is a continuing security investigation. We believe it is possible that this may be a matter of theft or deliberate destruction by a member of staff (either from Steria or IPS) rather than accidental loss but our investigation is still continuing and we have introduced additional safeguards. Until the issue is resolved, we are:
  - Increasing security cross-checks and audits to check number of applications in each box coming in and out of file holding and to ensure tally with system.
  - Changing processes and work patterns to reduce the number of people with access to file holding to a very small group and preventing access to those in support services that might normally require daily access.

Background on Security Procedures in place at File Holding:
The measures in place to protect information in file holding (as at the time of the incident) were as follows:

- Access controls in place and only staff with a need to access file holding for their job are permitted access. These are subject to regular review.
- All staff security cleared to CTC level in order to work in file holding (and anywhere in the examination and production environment).
- Boxes of applications are tracked through our system as they move through each step of processing in an office – including in and out of file holding.
- Security policies and procedures are in place that cover the correct way to handle data and a central security team conduct audits and investigations.
- All staff are also required to complete a mandatory e-learning package and pass a related test on data protection and handing which has been tailored to IPS specific situations.
- There is signage around the office to reinforce messages around the need to take care with personal information as well as to be careful about what is placed in confidential waste.

Risk Assessment and Mitigating Actions:
We have reviewed the impact of this incident on the basis of the potential harm to the applicants based on the sensitivity of the information and the volume involved in the incident using ICO guidance, especially the advice on data breach management and recently updated note on notification of breaches.

We developed an incident plan on the basis of the guidance, which outlines the steps we have taken so far and plan to take in the future (see Annex A for a summary).

Volume:
The volume of applications affected is small – 21 in total, affecting 35 people.

The ICO guidance notes that a loss of contact details relating to 1000 people would be considered a volume that would merit a formal breach notification. The Peterborough Regional Office handles approximately 1 million passport applications a year.

However, we recognise that even a small incident could be considered serious if the nature of the information affected were very sensitive

Sensitivity of the Information:
We reviewed this on the basis of whether this would result in private information becoming public and whether there was an exposure to identity theft.

Much of the biographical information included on the form is basic and commonly known data which is available in the public domain or from birth records.

The key risk identified lies around the exposure of the passport number and the old passport itself and whether that would result in potential for identity theft. However, we believe that the circumstances of the cases themselves and actions taken by us can mitigate any potential risk successfully.

Resulting Mitigating Actions:
- 14 of the passports involved were already expired and only 7 had any remaining validity. Physical security features on those passports themselves create additional barriers to the creation of an altered passport.
- As new passports have been issued and a passport number is product specific, the old passport number is out of date and the applicants will be using their new passports/passport numbers from now on.
- We have offered a free replacement passport to the parents and countersignatories whose passport details were included on a number of the applications as well. Thus, they will receive a new passport number which will invalidate the old number that was included on the application forms.
- In the same way as when a valid passport is lost or stolen we have cancelled the old passports and placed them on our lost/stolen database and stopfiles. We have also contacted Interpol, SOCA and CIFAS to inform them. This means that we can track the passport or passport number in question if anyone tries to use it to obtain a passport, cross borders, use to validate identity using the Passport Validation Service or if it is recovered by a third party.

Contact with Affected Individuals
We have proceeded to issue new passports to the applicants in question so they are not without a passport unnecessarily. We are now writing to these applicants to explain the incident has occurred and to apologise.

In addition, we are writing to relevant parents and countersignatories in question to inform them of the loss and to apologise. We have offered them a free replacement passport and a direct contact in the Peterborough office who will handle their application and can discuss any questions or concerns.

Lessons Learnt
We are in the process of conducting an investigation and a full “lessons learnt” exercise in the light of that investigation. These will be disseminated to all regional managers in our processing centres so actions are implemented across our network.

As the investigation concludes, we will inform the ICO of the outcomes and resulting actions.

Contact:
For further information about this report, please contact:

Duncan Hine
Executive Director of Integrity & Security
Identity & Passport Service
4th Floor Peel Building (SE Mailpoint D)
2 Marsham Street
London
SW1P 4DF

Tel: xxxxx xxxxxx
Email: duncan.hine@ips.gsi.gov.uk

Annex A: Action Plan

Containment & Recovery

Action	Status
Inform Steria manager and brief staff	Complete
Local search of office and bins	Complete
Cancel passports through lost/stolen route	Complete
Arrange central security intervention	Complete
Conduct central security search	Complete
Obtain and review access logs	Complete
Review access permissions	Complete
Revise access permissions and processes	Complete
Increase security auditing	Complete
On site central security interviews and review	Complete
Follow up analysis and further interviews	Complete
Report and establish new required actions from that point	Outstanding

Assessment of Ongoing Risk

Action	Status
Establish type of cases and supporting documents involved.	Complete
Conduct search to establish if information is still in office	Complete
Cancel passports through lost/stolen route and place information on stopfiles.	Complete
Issue new passports as requested to individuals	Complete

Notification of Risk

Action	Status
Contact ICO	Complete
Contact customers (incl. parents and countersignatories) when facts of case sufficiently established	Underway

Evaluation of Response:

Action	Status
Conduct a “lessons learnt” exercise to immediate response	Underway
Discuss with other regional managers, share action points and integrate into policy if required	Outstanding
Review if temporary security measures need wider application and assess if frequency of access control reviews need to be increased or process amended.	Outstanding