Office of the
Privacy Commissioner
of Canada

Privacy and Aviation Security:

AN EXAMINATION OF THE CANADIAN AIR TRANSPORT SECURITY AUTHORITY

**Audit Report of the
Privacy Commissioner of Canada**

Section 37 of the *Privacy Act*

FINAL REPORT

2011

Office of the Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 947-1698, 1-800-282-1376
Fax (613) 947-6850
TDD (613) 992-9190
Follow us on Twitter: @privacyprivee

© Minister of Public Works and Government Services Canada, 2011

Cat No. IP54-41/2011
ISBN 978-1-100-53856-3

This publication is also available on our website at **www.priv.gc.ca**.

Table of Contents

Main Points

WHAT WE EXAMINED

Various security and law enforcement organizations have a role in facilitating the safe and secure movement of air travellers. We assessed the personal information management practices of one entity: the Canadian Air Transport Security Authority (CATSA).

We reviewed CATSA's policies, practices and standard operating procedures, privacy impact assessments, security assessments and agreements with screening contractors. We also examined some of the technologies used to screen travellers, as well as the controls in place to protect personal information stored in electronic and hard copy format. In addition, we looked at an exploratory sampling of security incident reports and passenger complaint files.

Finally, we examined CATSA's overall privacy management framework, meaning the way in which it assigns privacy responsibilities, manages privacy risks and ensures compliance with its obligations under the *Privacy Act*.

WHY THIS ISSUE IS IMPORTANT

Tens of millions of passengers travel by air annually. Privacy rights in this context cannot be absolute. For example, it is widely accepted that consenting to searches is a prerequisite to boarding a flight, with the understanding that screening activities are undertaken to ensure the safety of passengers and crew. At the same time, measures designed to enhance aviation security should be necessary and reasonably proportionate to the threat in order that the privacy rights of individuals are not unjustifiably curtailed.

Several new technologies have been introduced by CATSA to facilitate the screening of passengers. These give rise to privacy concerns. There must be a level of assurance that the personal information derived from these technologies—and the other screening activities CATSA conducts—is limited to that which is legitimately necessary for aviation security, and that it is managed in accordance with the fair information practices embodied in the *Privacy Act*.

Implementing policies, procedures and controls to ensure personal information is appropriately protected is a critical element of sound privacy management. As an organization subject to the *Privacy Act*, CATSA has an obligation to implement safeguards to mitigate the risk of unauthorized or inappropriate access, use or disclosure of the personal information it collects while discharging its legislative mandate.

WHAT WE FOUND

CATSA has systems and procedures in place for managing personal information about air travellers. However, significant opportunities exist for CATSA to better manage privacy and achieve greater accountability, transparency and control over the information collected.

The *Canadian Air Transport Security Authority Act* empowers the Governor in Council to make regulations requiring CATSA to provide to the Minister such information as the Minister may request. The *Canadian Aviation Security Regulations* and the Security Screening Order impose certain reporting requirements on CATSA that authorize the collection of personal information under specific circumstances. We found that some of the personal information

collected by CATSA is unrelated to its mandate and beyond its legislative authority. This presents a risk to privacy by making available for use and disclosure passenger information that should not have been obtained.

As part of its pre-board screening activities and pursuant to regulated requirements, CATSA must verify the authenticity of boarding passes. The Boarding Pass Security System was introduced in 2009 to facilitate this process. The system captures the information that is recorded on the face of the boarding pass, as well as other data that is collected from the boarding pass bar code. Controls are in place to protect the data. Moreover, CATSA has demonstrated that the collection is necessary to fulfill its aviation security mandate, and the loss of privacy resulting from the collection is proportionate to the need. However, CATSA must take a more proactive role to achieve a higher degree of transparency regarding the collection, use and disclosure of personal information derived from boarding pass scanning technology.

While CATSA's use and disclosure practices generally comply with the *Privacy Act*, there is one notable exception. We found that personal information is disclosed if a large sum of money is fortuitously discovered in the baggage of or on an individual travelling domestically. The passenger's name and flight details are provided to police once the passenger has been screened and has left the screening area. It is not an offence to travel domestically with a large sum of money. CATSA does not ordinarily collect any personal information from an individual during the screening process. Therefore, information that would not otherwise be collected during the course of ordinary screening should not be collected to facilitate a disclosure to the police. Since the individual is permitted to proceed through screening, it is evident that the discovery of money does not constitute a threat to aviation security and therefore is outside of CATSA's mandate.

Various technologies are used to screen passengers. Full-body image scanners are present in many Canadian airports. The technology penetrates the clothing of a traveller to reveal a body image in order to detect explosives or non-metallic weapons. CATSA has implemented controls to ensure that an image cannot be linked to a name or any other identifiable information about the passenger. Moreover, we tested full-body scanners during our site visits and confirmed they are configured so that images cannot be retained and cannot be printed, and images are permanently deleted once the passenger has been screened. While the security framework surrounding the technology is sound, procedures designed to protect privacy are not consistently followed, thereby placing images—and potentially the identity of the passenger—at risk of exposure.

Maintaining the security of personal information is an essential component in meeting the protection requirements established under the *Privacy Act*. We found deficiencies during our site visits to airports where we observed security incident reports containing travellers' personal information stored on open shelving units, on the floor and in cabinets that did not meet required security specifications. At one airport, we found security incident reports stored in boxes in a room used to conduct private searches. We also found weaknesses in certain disposal practices.

CATSA has outsourced passenger screening to 11 private sector companies. Contracting out a program or service-delivery function does not relieve an institution from its obligations under the *Privacy Act*, associated regulations and related Treasury Board Secretariat policies and directives. Compliance monitoring is essential for any outsourcing arrangement that involves personal information. CATSA has not exercised due diligence in this regard. It has been guided by the assumption that screening contractors are managing passengers' personal information appropriately, without any assurance that this is so. An ongoing monitoring strategy,

including audits, would provide a means of mitigating privacy risks and provide a level of assurance that fair information practices are integrated into CATSA's day-to-day operations.

Finally, while core elements of a privacy management framework are in place, we found gaps that need to be addressed. Specifically, there is a lack of privacy-specific training for staff and a privacy breach protocol has not been formalized. In addition, CATSA has not accounted for and described its categories of personal information in *Info Source*, a Treasury Board Secretariat publication that informs the public of what information is held by the government, how it is managed and how individuals may access their personal information.

CATSA has responded to our findings. Its responses follow each recommendation throughout this report.

Introduction

1. Canada's aviation security system involves many agencies with differing mandates and authorities. It includes policing, intelligence, physical security and technology to minimize risks. Many organizations have a role to play. Transport Canada is the policy-maker and regulator responsible for enforcing aviation security regulations. The RCMP and local police, airport authorities and air carriers all contribute to the protection of the general public, passengers, airline crew members, airport employees and aviation facilities.

2. The Government of Canada has re-evaluated the aviation security program on a number of occasions, most notably following the bombing of Air India Flight 182 in 1985 and subsequent to the terrorist attacks on September 11, 2001. In response to the latter, the Budget of 2001 allocated $2.2 billion over five years to improve airport security and screening.

3. Security and privacy objectives are often perceived as values to be balanced against each other where, for example, increased security must result in a corresponding loss of privacy. However, a strong control framework over the management of personal information will mitigate privacy risks and will also support aviation security objectives.

ABOUT THE AUDIT ENTITY

4. The Canadian Air Transport Security Authority (CATSA) was established as a Crown corporation in April 2002. Its creation was a key component of the Government of Canada's response to the events of September 11, 2001.

5. CATSA's responsibilities fall into four air security areas, the most visible of which is the pre-board screening of passengers for prohibited items (a full list of prohibited items is found in Appendix B). The screening process involves metal detection, X-ray technology, explosive trace-detection equipment, physical searches and, in some cases, full-body imaging. Other mandated activities include screening non-passengers (e.g., flight crews, baggage handlers and airport maintenance staff) and managing the Restricted Access Identity Card Program, a biometric identification program for non-passengers accessing restricted areas of airport terminals.

6. CATSA reports to Parliament through the Minister of Transport. As of March 31, 2010, it had a staff complement of 530 employees, 6,790 screening officers (contract personnel) and an annualized budget of $585.9 million.[1] More information about CATSA is available on its website at **www.catsa-acsta.gc.ca**.

[1] Canadian Air Transport Security Authority Annual Report, 2010, pp.14, 44 (www.catsa.gc.ca/File/Library/87/English/AnnualReport2010.pdf).

FOCUS OF THE AUDIT

7. The audit focused on the management of personal information about air passengers. The objective was to assess whether CATSA has implemented adequate controls to protect passengers' personal information, and whether its policies, procedures and processes for managing such information comply with the fair information practices embodied in sections 4 through 8 of the *Privacy Act*.

8. The audit did not include a review of CATSA's handling of personal information about its employees or contract screening officers, nor did it examine the organization's non-passenger screening and restricted area identity card system processes. Further, while the review included an assessment of the controls surrounding various screening technologies and databases, the audit was not designed to examine CATSA's overarching information technology infrastructure. Information on the scope, criteria and approach can be found in the **About the Audit** section of this report.

Observations and Recommendations

COMPLIANCE WITH THE CODE OF FAIR INFORMATION PRACTICES

9. The *Privacy Act* sets out the rules governing the management of personal information held by federal government institutions. Sections 4 through 8, which are commonly referred to as the Code of Fair Information Practices, restrict the collection of personal information and limit how that information, once collected, can be used and disclosed. The Code balances the legitimate collection and use requirements essential to government programs with an individual's right to a reasonable expectation of privacy.

Some collection activities extend beyond legislative authority

10. Within the federal context, section 4 of the *Privacy Act* establishes criteria for the collection of personal information. Specifically, the collection must relate directly to an operating program or activity of the government institution. The Treasury Board Secretariat has advised departments as follows:

> The [*Privacy Act*] states that government institutions shall not collect personal information unless it relates directly to an operating program or activity. The policy requires that institutions have administrative controls in place to ensure that they do not collect any more personal information than is necessary for the related programs or activities. This means that institutions must have parliamentary authority for the relevant program or activity, and a demonstrable need for each piece of personal information collected in order to carry out the program or activity.

11. Institutions are required to establish mechanisms to ensure that they do not collect more personal information than is necessary. In other words, there must be a demonstrable need for each piece of information collected. We expected to find that CATSA's collection activities were both relevant and not excessive.

12. We interviewed staff and reviewed standard operating procedures. We also examined an exploratory sampling of security incident reports.

13. **The authority to collect personal information.** The *Canadian Aviation Security Regulations* (the Regulations) impose certain reporting requirements on CATSA, air carriers and aerodrome operators. CATSA has cited the Regulations as its primary authority for collecting personal information about air travellers. It also relies upon the Security Screening Order for certain collection practices. The Order stipulates that CATSA must retain a record of all instances in which explosive detection trace equipment alarms are triggered, and make this record available to the Minister of Transport.

14. The Regulations require CATSA to immediately notify the appropriate air carrier, aerodrome operator, police service and the Minister of Transport if certain weapons, explosives or incendiary devices are detected in the course of screening travellers and their baggage. The appropriate air carrier, aerodrome operator and the Minister must also be notified of any other aviation security incident that involves a peace officer at a restricted area access point or in any other part of an aerodrome where it conducts screening.

15. The Regulations do not specifically define what type of incident might constitute "any other aviation security incident." However, Transport Canada has advised air carriers and aerodrome operators as follows:

> An "aviation security incident" is defined as an actual, attempted, threatened or suspected unlawful act which would result in the interference, a breach or malfunction of the civil aviation security system. Such incidents include but are not limited to: hijackings, attempted hijackings, explosions, the discovery of weapons, explosive substances or incendiary devices and specific threats against the aerodromes or air carriers.[2]

16. **CATSA's collection practices.** We found that CATSA collects a passenger's personal information when the following are discovered during the security-screening process:

- prohibited or concealed items that pose or initially appear to pose a threat to aviation security;
- contraband (including illegal narcotics) or items appearing to be contraband; and
- a large sum of money carried by a passenger in respect of which it is reasonable to conclude is greater than $10,000.

17. CATSA also collects personal information about uncooperative or unruly passengers. Various indicators are used to assess a passenger in this regard, including when physical harm to a person or property has occurred or a person threatens to cause serious harm to a screening officer or others. Passengers who display such conduct at a screening point may exhibit similar behaviour in flight; therefore, they are deemed to pose a potential threat to aviation safety. The decision to permit or deny the person boarding ultimately rests with the air carrier.

18. The discovery of a prohibited item during the screening process can clearly be described as an aviation security incident. An unruly passenger who is deemed to pose a potential security threat would be categorized in the same way. Accordingly, the collection of personal information is authorized and is necessary for CATSA to meet its reporting obligations and discharge its mandate. However, this would not apply to most "false positive" situations where a perceived threat to aviation security is determined to be non-existent after further examination and/or police intervention. In such cases there is no threat and, therefore, no necessity to collect personal information for reporting purposes.

19. **Certain collection activities are unrelated to aviation security.** CATSA does not have the authority to collect personal information for general law enforcement investigative purposes. It is not a police organization and it is not empowered to act as an agent of the police in this regard. However, we found personal information in CATSA's files that was collected for such purposes.

20. As reported in paragraph 16, CATSA collects passenger information when it fortuitously discovers contraband, suspected contraband and large sums of money. When discoveries are made, CATSA's standard operating procedures stipulate that certain action be taken, including notifying the police. The Canada Border Services Agency (CBSA) is contacted when the currency is carried by or in the baggage of an individual taking an international flight.[3]

21. CATSA was unable to demonstrate that passengers carrying large sums of money or narcotics on an aircraft were a threat to aviation security. If these items are fortuitously discovered, CATSA screening officers may notify law enforcement officials. Once the police and/or the CBSA have been summoned, CATSA's involvement ends. As

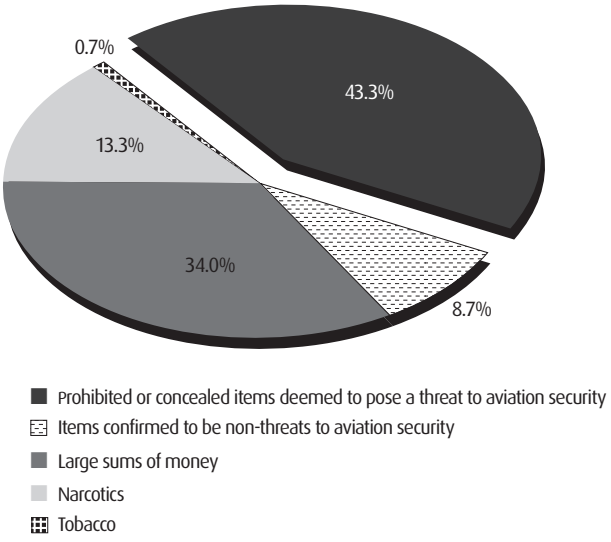
[2] Reporting Procedures for Security Incident, AB-2500-4-20, 2005.11.30 (www.tc.gc.ca/eng/civilaviation/opssvs/nationalops-caco-incident-procedures-730.htm).

[3] *Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, it is an offence to import or export currency over $10,000 without notifying customs officials.

an aviation security incident has not occurred, CATSA should not collect any personal information about the passenger.

22. The audit also revealed that CATSA collects personal information about domestic travellers carrying large sums of money. The screening officer records the passenger's name and flight details, completes the screening process and provides the recorded information to the police once the passenger has left the area. As CATSA permitted these individuals to proceed through screening with the funds in question, it is evident that the discovery of these items does not constitute a threat to aviation security.

23. We found that CATSA has over 10,400 incident reports on file. We randomly extracted an exploratory sample of 150 reports for examination. Over half of the reports—approximately 57 percent—concerned matters unrelated to aviation security, including the discovery of narcotics, tobacco and large sums of money. An overview of incident type (item found) is provided below.



24. On the basis of our review, we conclude that CATSA is collecting personal information that falls outside its legislative mandate. Due to the size of our audit sample, it is not known to what extent CATSA's information holdings contain reports that should not be there.

25. RECOMMENDATION

CATSA should implement measures to ensure that the collection of personal information (PI) is limited to aviation security incidents.

CATSA's response:

CATSA agrees to implement measures to ensure the collection of PI is limited to aviation security incidents.

With respect to situations involving Explosive Detection Trace (EDT) alarms, CATSA is required by the Security Screening Order (SSO) to keep a record of every instance in which this alarm is triggered. CATSA will consult with Transport Canada to confirm what types of information are necessary to meet the reporting requirements of the SSO.

The collection of personal identifiers from the boarding pass bar code is justified

26. As part of the pre-board screening process and pursuant to regulated requirements, CATSA must verify the validity of boarding passes. The verification is generally limited to a visual confirmation that the date, airport terminal and gate identified on the document are valid. As this method cannot detect boarding passes that have been altered or duplicated, CATSA introduced the Boarding Pass Security System (BPSS) in 2009. At the time our work was completed, BPSS technology was in use at seven of Canada's major airports.[4]

[4] Airports located in Halifax, Montreal, Ottawa, Toronto, Calgary, Edmonton and Vancouver. BPSS has not been deployed at the James Armstrong Richardson International Airport in Winnipeg.

27. We examined BPSS policies, internal processes and interviewed staff responsible for operating the system. We also observed the use of the technology during our site visits. We expected to find that the collection of personal information was necessary to verify the validity of a boarding pass and thereby prevent an individual from gaining inappropriate access to a secure area of an airport.

28. In an airport that uses this technology, a boarding pass is scanned twice: initially by a CATSA officer (using a hand-held device) when a passenger enters the screening queue, and then again by a stationary device prior to the X-ray machines. The results are displayed on a monitor visible to the screening officer. In addition to displaying the information contained in the boarding pass bar code, the authenticity of the boarding pass is verified and confirmation is provided as to whether it was previously scanned.

29. The BPSS scan captures the same information that is recorded on the boarding pass, including: passenger name, priority status, air carrier, departure date and time, gate and seat number. It also captures other bar code data, such as class/cabin and record locator number. Once a boarding pass is scanned, the BPSS records the scan date and time, the checkpoint and waiting time.

30. Although the BPSS was implemented to detect fraudulent boarding passes, CATSA is using the data (specifically passenger names) to respond to security incidents and security breaches,[5] as well as passenger claims and complaints. CATSA explained that the name, along with closed-circuit television (CCTV) footage, is used to quickly locate the individual and resolve the security incident or breach. Having a passenger's name also expedites the processing of claims and complaints by establishing the specific time and screening line used to process the passenger. Without the name, CATSA is required to conduct an extensive search of CCTV footage, which may compromise the resolution of aviation security incidents.

31. A traveller's personal information (see paragraph 29) is held in the BPSS database for 30 days. If the information is used to resolve an incident, security breach or passenger complaint, it is retained for a minimum of two years. We found there are adequate controls to protect the data (addressed in paragraphs 66 through 70 of this report).

32. As a general rule, personal information should not be collected on the basis that it may have a future use. Such a practice is not in keeping with the limiting collection principle. CATSA has demonstrated that the collection of personal information from a passenger's boarding pass is necessary to fulfill its aviation security mandate, and the loss of privacy resulting from the collection is proportionate to the need. We also found the 30-day retention period for such data to be reasonable. However, we did note that passengers are not informed of this retention period, or that BPSS data may be shared with CATSA's foreign counterparts to address matters relating to aviation security.

[5] A security breach is when a person or item has entered the restricted area without being fully screened.

33. RECOMMENDATION

CATSA should more clearly inform passengers of the purposes for which BPSS data is collected, the uses that are made of it, to whom and under what circumstances the information may be shared with third parties, and how long the data is kept.

CATSA's response:

CATSA agrees and will ensure that passengers are properly informed of the purposes for which BPSS data is collected, the retention period and potential disclosures. This information will be included in a new privacy notice to be distributed by December 1, 2011 at locations where BPSS is deployed. CATSA will also continue to work collaboratively with the Treasury Board Secretariat to ensure that BPSS information is accurately described in the next edition of *Info Source*.

Use and disclosure practices generally comply with the *Privacy Act*

34. Sections 7 and 8 of the *Privacy Act* govern the use and disclosure of personal information. In general terms, government institutions can use the information only for the purposes for which it was collected, or for a use consistent with that purpose. It may also disclose the information for the same purposes. There are other circumstances under which personal information may be disclosed without the individual's consent,[6] including where the disclosure is authorized under an Act of Parliament or regulation.

35. We expected to find that CATSA's disclosure practices were in compliance with the *Privacy Act*. We examined its pre-board screening processes and standard operating procedures, interviewed staff and examined a sampling of incident reports.

36. CATSA has specific reporting requirements under the *Canadian Aviation Security Regulations* (the Regulations) and the Security Screening Order. For example, if explosive substances, incendiary devices, prohibited or loaded weapons are detected, CATSA must, pursuant to the Regulations, notify the appropriate air carrier and police service, the aerodrome operator and the Minister of Transport. This also applies to any other aviation security incident that involves a peace officer where the screening is conducted.

37. Searching for contraband is beyond the legislated mandate of CATSA. However, as noted previously, it will contact the police when contraband (e.g., illegal narcotics), large sums of money and other suspicious items are fortuitously discovered during the screening process. We were told that the passenger's name, boarding information and a description of the item(s) found are disclosed. The information is provided immediately, so the police may intervene to address the matter or, in the case of a domestic traveller carrying a large sum of money, after the passenger has proceeded through the screening process. CATSA also notifies the Canada Border Services Agency (CBSA) when currency in an amount greater than $10,000 is discovered on a passenger travelling internationally.

38. The disclosure of personal information with respect to the discovery of contraband and large sums of money cannot be viewed as a disclosure for the purpose of aviation security. Furthermore, the Regulations and Security Screening Order do not require CATSA to report such incidents.

[6] Subsection 8(2) of the *Privacy Act* sets out 13 categories of permissible disclosures.

39. Under the *Privacy Act*, non-consensual disclosure of personal information is not permitted, except in accordance with the exceptions Parliament has identified in section 8 of the Act. CATSA's governing legislation and regulations do not authorize the disclosure of this information and travellers' personal information is not collected by CATSA for the purpose of making disclosures to the police. As a result, CATSA's authority to disclose the personal information of air travellers to police depends on whether such disclosures can be considered a use consistent with the purpose for which the information was obtained.

40. With respect to consistent uses, the Treasury Board Secretariat provides the following guidance:

> For a use or disclosure to be consistent, it must have a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled.
>
> A test of whether a proposed use or disclosure is "consistent" may be whether it would be reasonable for the individual who provided the information to expect that it would be used in the proposed manner. This means that the original purpose and the proposed purpose are so closely related that the individual would expect that the information would be used for the consistent purpose, even if the use is not spelled out.

41. CATSA obtains personal information for the purpose of screening individuals and their baggage for prohibited items and threats to aviation security. The intended use of the information disclosed to the police and the CBSA is for general law enforcement and possibly prosecution. Determining whether this is a consistent use requires an assessment of whether individuals can reasonably expect that CATSA will notify the police and/or the CBSA where a person or baggage is searched for purposes within CATSA's mandate, but items that are inadvertently discovered fall outside of that mandate.

42. Individuals have a reduced expectation of privacy in an aviation security environment. Searches in an airport setting are anticipated; passengers expect that both they and their baggage will be screened and potentially searched. We have considered CATSA's mandate and the reasonable expectation of privacy in an airport security context.

43. In our view, it is reasonable for an individual to expect that CATSA would notify the appropriate authorities when illegal items—or items appearing to be illegal—are inadvertently discovered. While individuals are only consenting to a search of their person and baggage for aviation security purposes, it would be unreasonable to expect that clear evidence of contraband and other illegal items would be ignored. This would also apply to the exportation of an amount of currency in respect of which it is reasonable to conclude is greater than $10,000, without undertaking an investigation to support the conclusion.

44. Where the discovery is inadvertent and unintended, notifying the police and/or CBSA has a reasonable and direct connection to the original purpose for which the information was obtained—that is, for public safety and ensuring compliance with the law in the aviation security context.

45. However, a disclosure relating to a large sum of money carried by a domestic traveller cannot be considered a consistent use. It is not an offence to travel domestically with a large sum of currency. It would rarely, if ever, be apparent to CATSA officials that the money may constitute evidence of a crime. Additional investigation would be required to make such a determination, something that exceeds CATSA's expertise and mandate.

46. CATSA does not ordinarily collect any personal information from an individual subject to screening. Therefore, information that would not

otherwise be collected during the course of ordinary screening should not be collected to facilitate a disclosure to the police. Since the individual is permitted to proceed through screening, it is evident that the discovery of money does not constitute a threat to aviation security and, therefore, is outside of CATSA's mandate.

47. We also found that CATSA provides personal information to airline carriers regarding incidents unrelated to aviation security. The information is disclosed verbally. While it may be appropriate to notify an airline if a passenger will be delayed beyond a flight's departure time, there is no requirement to disclose specifics (e.g., contraband was found in the traveller's baggage and the individual has been detained by the police). CATSA officials informed our office there have been occasions when specific details have been shared with airline officials.

48. RECOMMENDATION

CATSA should:

- cease the practice of notifying police when it discovers a large sum of money in the baggage of or on an individual travelling domestically; and
- ensure that all disclosures to airline carriers are limited to only that which is necessary in the circumstances of each case.

CATSA's response:

CATSA agrees and will implement the recommendation. Amendments to CATSA's Standard Operating Procedures (SOPs) will be included in the next release, scheduled for early in the third quarter of 2011–12.

Personal information is retained longer than necessary

49. Fundamental to privacy is the principle that personal information should only be obtained if there is a legitimate and authorized need. Under the *Privacy Act*, collection must be relevant to an operating program or activity. Relevance is determined by statutory authority.

50. As reported previously, CATSA is collecting personal information that exceeds its aviation security mandate and, therefore, is beyond its statutory authority. Any collection beyond statutory authority contravenes the limiting-retention principle. In other words, if an institution doesn't have the authority to collect personal information, it shouldn't keep it. This presents a risk to privacy by making available for use or disclosure personal information that should never have been obtained.

51. The *National Archives Act* and the policy on the Management of Government Information Holdings require federal institutions to develop retention and disposal schedules to manage their records. These schedules establish how long records will be kept before they are destroyed or transferred to the control of Library and Archives Canada. The Librarian and Archivist of Canada issues Records Disposition Authorities for this purpose.[7]

52. When an incident occurs, passenger information collected during the screening process is generally recorded on a security incident report. The report typically includes the passenger's name, flight information, address, telephone number and a summary of events (details surrounding the security incident or breach). The report is faxed to CATSA's Security Operations Centre in Ottawa. It is then entered into the Call and Incident Data Collection System, the electronic repository for security incident reports.

[7] A Records Disposition Authority does not constitute a requirement to destroy records; it permits the destruction of documents that do not need to be preserved for future archival or historical use.

53. We expected to find that CATSA had a retention and disposal schedule for the personal information collected under its control, with complementary processes and procedures. We found that a schedule has not been established; as a result, security incident reports are kept at CATSA's head office indefinitely.

54. A records retention and disposal schedule is important from a privacy perspective. It provides a mechanism for ensuring that non-archival and non-historical personal information is destroyed when it is no longer required. Any further retention may result in prejudice against the individual to whom the information relates.

55. RECOMMENDATION

CATSA should permanently delete all personal information held in its information holdings (electronic and hard copy records) that it does not have the authority to collect, specifically records capturing the fortuitous discovery of:

- contraband, including illegal narcotics;
- items that are initially perceived to pose a threat to aviation security and the threat is determined to be non-existent after further examination and/or police intervention;
- items that appeared to be illegal and required investigation beyond CATSA's mandate and expertise; and
- large sums of money carried by or in the baggage of passengers.

CATSA should also consult with Library and Archives Canada to establish a records retention and disposal schedule for personal information collected under its aviation security mandate.

CATSA's response:

CATSA agrees and will implement these recommendations. An action plan will be developed.

SAFEGUARDING PASSENGERS' PERSONAL INFORMATION

56. Maintaining the security of personal information is an essential component in meeting protection requirements established under the *Privacy Act*. Appropriate measures and controls must be present to ensure personal data is not subject to unauthorized access, use, disclosure, alteration or destruction.

57. Treasury Board Secretariat policy establishes baseline (mandatory) security requirements to protect and preserve the confidentiality and integrity of government assets, including personal information. Federal departments and agencies are responsible for conducting their own assessments to determine whether safeguards above baseline levels are necessary.

58. We expected to find adequate physical, technical and administrative controls to protect passengers' personal information. We examined CATSA's procedures, processes, system access controls and contracts with third-party service providers.

59. We found that CATSA's computer and video systems operate on a secure network that connects its head office, airports and data centres. We reviewed the network architecture and found adequate measures to protect personal information. These include firewalls, intrusion detection and prevention, automated software patch management and access controls. Threat and Risk Assessments have been completed and annual penetration tests are performed to identify and remedy potential weaknesses.

Security framework surrounding full-body scanning technology complies with Canadian privacy law

60. At the time of our audit, CATSA had implemented full-body scanning (FBS) technology at 23 Canadian airports. The technology penetrates the clothing of travellers to reveal images of the body in order to detect explosives or weapons that might otherwise be undetectable. It works by projecting low-level radio frequency (RF) energy over and around the passenger's body. The RF wave is reflected back from the body and from objects concealed on the body, producing a three-dimensional image.

61. We examined FBS system configurations during our site visits and observed the physical and technical safeguards in place to manage the images. CATSA has established a strong framework to protect passengers' privacy, key elements of which are:

- controls to ensure it is not possible to correlate an FBS image with the name of the passenger to whom it belongs or any other identifying information;
- scanned images are sent electronically to a remote viewing room to ensure the screening officer cannot view or identify the passenger;
- the images cannot be retained;
- the scanned image is permanently deleted immediately after the screening is complete;
- transitory images captured by the technology cannot be accessed by or transmitted to a remote location; and
- full-body scanned images cannot be printed.

62. While a sound IT control framework exists to protect FBS images, procedures designed to mitigate certain privacy risks are not consistently followed. These procedures place restrictions on who may enter the FBS image viewing room, when it can be entered and exited, and the items permitted inside.

63. The procedures stipulate that the screening viewing officer must ensure the FBS image is cleared from the screen before any person enters or exits the room. We observed instances of non-compliance with this requirement. We also noted an official inside the image viewing room with a cell phone; cell phones and smart phones are strictly prohibited because of their recording capabilities.

64. We also located a closed-circuit television camera in the ceiling of the FBS viewing room at one airport. The camera was disabled after we brought the matter to CATSA's attention.

65. RECOMMENDATION

Given the privacy concerns surrounding the use of full-body scanning technology, CATSA should:

- ensure that procedural safeguards to protect privacy are understood, enforced and subject to ongoing compliance monitoring; and
- conduct a physical inspection of all full-body scan viewing rooms and disable any closed-circuit television installations.

CATSA's response:

CATSA agrees. As a result of an earlier consultation with the Office of the Privacy Commissioner of Canada, privacy safeguards were put in place. CATSA will continue to ensure that established safeguards are understood and adhered to by all employees, screening contractors and screening officers. CATSA will issue a shift briefing to remind screening personnel of the established SOPs for full-body scanners. Additionally, CATSA will inspect all full-body scanner deployments to ensure that all privacy safeguards are respected. Both activities will be completed in the third quarter of 2011–12.

The observation regarding the CCTV camera was an isolated incident and has been corrected.

Safeguards are in place to protect passengers' boarding pass information

66. CATSA has deployed the Boarding Pass Security System (BPSS) in seven of Canada's major airports. Responsibility for managing the system has been outsourced to a third-party service provider.

67. We expected to find measures to protect boarding pass information that is transmitted to and stored in the BPSS. We examined system design and network documentation, system configuration settings and physical controls. We also reviewed the contract between CATSA and the third-party service provider.

68. We found the data extracted from a boarding pass bar code is transmitted by a secure network to a local server, and then to a central database. CATSA has implemented controls to protect data in transmission. Moreover, the personal information stored in the database is encrypted.

69. We also found that the third-party service agreement includes sound privacy provisions, including:

    - personal information must be stored in Canada;
    - security and physical measures must be in accordance with Government of Canada security standards;
    - the information cannot be used for secondary purposes; and
    - any individual with access to the database must have a Secret security clearance.

70. Although responsibility for managing the BPSS has been outsourced, CATSA has retained control over issuing access rights to the system. As well, data retention periods and system configuration settings are controlled by CATSA.

Personal information captured by closed-circuit television is tightly controlled

71. CATSA has installed closed-circuit television (CCTV) to record the movement of passengers from the time they enter the screening queue (waiting line) until they have been processed by screening officers. The technology is also used to respond to security incidents and breaches, as well as passenger claims and complaints.

72. We found there are appropriate controls over access to, use and disclosure of CCTV footage. The technology is managed by the Security Operations Centre at CATSA's head office. Live CCTV feeds can only be viewed at the Centre. Footage is retained for a period of 30 days at two secure locations, at which time it is overwritten. If required, extracted footage may be viewed by airport screening officials through a software application. Access to the footage is tightly controlled and restricted to authorized personnel. Moreover, CATSA officials informed us that it will not release a copy of CCTV footage unless compelled to do so under a warrant or court order.

Risks associated with passenger database have not been fully assessed

73. The Call and Incident Data Collection (CIDC) System is the electronic repository for passengers' personal information. We expected that all privacy risks associated with the system had been identified and addressed.

74. Controlled access to an information technology (IT) system and its data represents a key safeguard because it restricts the use and disclosure of personal information to those who have a legitimate need to know. An effective method of mitigating the risk of data being compromised is to limit access rights to the system. This is commonly referred to as "role-based access." We examined a listing of CIDC users by role. Access rights were in keeping with the need-to-know principle, with one exception. We noted that software developers are granted access to passenger information; such access is not required to fulfill their CIDC support function.

75. Although access rights are well managed, CATSA has not fully assessed the risks surrounding the system. The Treasury Board Secretariat's Management of Information Technology Security

Standard requires federal organizations to certify and accredit an IT system prior to approving it for operation. Certification verifies that mandatory security requirements for an IT system are applied. It also verifies that controls and safeguards to protect data are functioning as intended. Accreditation signifies that management has authorized operation of the system and has accepted any residual risk.

76. CATSA was unable to demonstrate that the CIDC system was subject to a formal certification and accreditation process, as required by the Treasury Board Secretariat's security standard. This exposes CATSA to a risk that the system could have undetected security weaknesses, which may affect the integrity of the personal information residing in it.

77. RECOMMENDATION

CATSA should subject the Call and Incident Data Collection (CIDC) System to a formal certification and accreditation process.

CATSA's response:

CATSA agrees. The CIDC system has been replaced by a new system called the Service Monitoring and Recording Toll (SMART). CATSA will be certifying and accrediting the new system in-house. The accreditation authority for SMART will be the Program/Service Delivery Manager.

Passengers' personal information is not always stored securely

78. The Treasury Board Secretariat's Operational Standard on Physical Security provides mandatory requirements to counter threats and risks to personal information. We expected to find that the physical safeguards to protect passenger data were commensurate with the sensitivity of the personal information. We looked at CATSA's physical security controls for safeguarding passenger information, agreements with its screening contractors and observed storage practices during our site visits.

79. CATSA's head office and the information stored within are controlled by various measures, including security guards, CCTV cameras and an intrusion-detection alarm system. Electronic access control cards, biometric identifiers and security cabinets are among the measures used to restrict access to the premises and records. These measures are complemented by CATSA's clean desk policy and regular security inspections. We found no evidence to suggest personal information could be compromised because of inadequate physical security controls.

80. Areas requiring improvements were noted during our site visits to airports. CATSA has outsourced passenger screening to 11 private sector companies. Each contract includes a confidentiality agreement. The agreement establishes the contractors' obligations in terms of safeguarding passenger information. It stipulates that sensitive information must be protected in a manner consistent with government security policy. We found deficiencies in this regard; we observed security incident reports on open shelving units, on the floor and in cabinets that did not meet required security specifications. At one airport we found security incident reports stored in boxes in a room used to conduct private searches on passengers.

81. The confidentiality agreement requires screening contractors to protect records in accordance with CATSA's Document Protection Procedures. These procedures outline the storage and transmission requirements for Protected and Secret information. The agreement stipulates that CATSA will identify all information falling within either of the two categories. CATSA has not done so, either on the security incident reports or in its standard operating procedures. The absence of a security designation on passenger records may be a contributing factor to some of the storage deficiencies we observed.

82. RECOMMENDATION

To meet Treasury Board Secretariat requirements and ensure passenger information is adequately protected, CATSA should apply a security designation that is commensurate with the sensitivity of the information. It should also ensure that:

- the designation is marked on the information and is reflected in CATSA's standard operating procedures; and
- screening contractors implement physical security measures that comply with Treasury Board Secretariat standards.

CATSA's response:

CATSA agrees. In July 2011, CATSA issued a new directive (Directive #56) to all screening contractors. This directive highlights the importance of handling information properly; provides guidance about the types of information that require special handling that they are most likely to see; and indicates how to store, transmit and destroy documents containing these types of information. A further update to this directive will be provided to screening contractors as a reminder to follow the retention periods listed on the forms where PI is collected.

Audit criteria regarding the management of passenger PI by screening contractors will be added to CATSA's airport audit program in the fourth quarter of fiscal year 2011–12.

Weaknesses in certain disposal practices pose a significant privacy risk

83. Section 6(3) of the *Privacy Act* requires government institutions to dispose of personal information in accordance with the Regulations and with any directives or guidelines issued by the Treasury Board Secretariat. The Secretariat's Operational Security Standard on Physical Security provides minimum requirements to ensure protected and classified records are destroyed in a secure manner. These requirements are intended to make the reconstruction of information on shredded paper impractical.

84. Treasury Board Secretariat policy establishes a strip-cut to a maximum width of 3/8 inch (10 mm) as the minimum shredding standard for information designated as Protected A or Protected B. We expected to find that CATSA's disposal practices met or exceeded the minimum shredding standard, with a mechanism that provided assurance that the standard was consistently applied. We examined procedures surrounding the destruction of incident reports and received briefings on screening contractors' off-site disposal practices.

85. We found that security incident reports are retained at CATSA's head office indefinitely. Consequently, our inquiries focused on the destruction of records by screening contractors. We were told that copies of incident reports are held by contractors for one year, at which time they are destroyed.

86. The contracts and confidentiality agreements with screening providers are silent on disposal requirements, and CATSA's standard operating procedures provide little guidance in terms of ensuring records are destroyed in a manner that respects privacy. As a result, it is left to the screening contractor to develop, implement and manage the disposal process. This has included establishing arrangements with private sector shredding companies when such services are required.

87. The screening contractors at three of the airports visited use on-site shredders to destroy records. We collected a sample of shredded material at one of the sites. As the exhibit reflects, the results fall short of the Treasury Board Secretariat's maximum 3/8 inch shredding standard. While there is insufficient evidence to suggest this is representative of a systemic problem, it does underscore the importance of monitoring disposal practices.

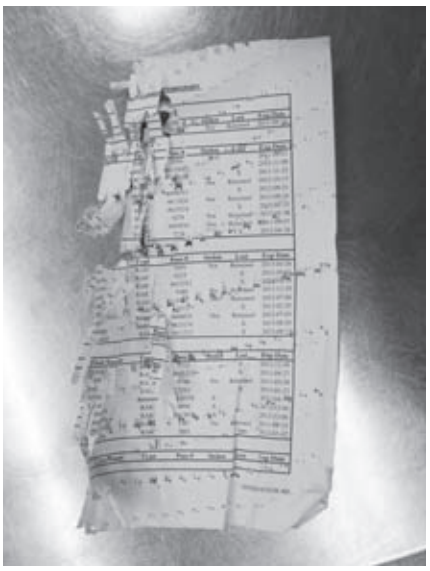


Exhibit 1: Sample of shredded material

88. We also found weaknesses in the management of certain outsourcing arrangements. Some of the contractual agreements with private shredding companies are established and managed by screening contractors. CATSA is not a party (signatory) to the contracts and it does not review the agreements to verify that they satisfy Government of Canada contracting requirements.

89. We also noted an absence of monitoring activity to ensure screening contractors were destroying passenger information in a secure manner. We expected to find an audit protocol for contracts governing off-site records destruction, with supporting documents to demonstrate CATSA systematically monitors contracted shredding companies through periodic inspections and audits. Such a protocol does not exist. As a result, there is no assurance that:

- individuals handling passenger information are security-screened to the appropriate level;
- incident reports are destroyed in a manner such that they cannot be reconstructed; and
- records are disposed of on a timely basis to mitigate the risk of unauthorized access.

90. Compliance monitoring is critical for any outsourcing arrangement that involves personal information. CATSA has not exercised due diligence in this regard. It assumes that off-site disposal practices comply with Treasury Board Secretariat requirements without any assurance this is so. This poses a significant privacy risk.

91. RECOMMENDATION

CATSA should:

- ensure that all contracts related to the disposal of personal information collected under its legislative mandate comply with Treasury Board Secretariat requirements;
- implement a protocol for monitoring off-site destruction practices; and
- ensure off-site destruction contracts include a requirement that the service provider issue a certificate of destruction recording the date records are destroyed and the name of the authorized officer who conducted or witnessed the destruction.

CATSA's response:

CATSA agrees. Provisions governing the proper disposal and off-site destruction of passenger PI will be written into the new airport screening-services agreements to be implemented as of November 1, 2011.

In addition, as noted in CATSA's response to the preceding recommendation (paragraph 83), in July 2011, CATSA issued a new directive (Directive #56) to all screening contractors. The directive highlights the importance of handling information properly, provides guidance to screening contractors about the types of information requiring special handling that they are most likely to see, and indicates how to store, transmit and destroy documents containing these types of information.

Audit criteria regarding the management of passenger PI by screening contractors will be added to CATSA's airport audit program beginning in the fourth quarter of 2011–12.

PRIVACY MANAGEMENT AND ACCOUNTABILITY

92. A privacy management framework refers to the controls in place, including policies and procedures, to ensure personal information is managed appropriately. Core elements of a framework include identification and management of privacy risks, a privacy breach protocol, compliance monitoring, employee awareness training and accountability for privacy.

93. CATSA has implemented a suite of standard operating procedures to manage its personal information holdings. We examined these procedures and CATSA's security and information management policies. We identified both sound privacy practices and opportunities for improvement.

Privacy risk management process is in place

94. In 2002, the Treasury Board Secretariat introduced a policy on Privacy Impact Assessments (PIAs) to ensure privacy principles were considered for all new or substantially redesigned programs and services. The policy was replaced with a PIA Directive in April 2010. The extent to which departments are compliant with the directive is dependent on the framework in place to report on activities that may require privacy impact analysis.

95. We asked CATSA how and when it determines whether a PIA is required. We were told that any change in the IT infrastructure would immediately trigger a PIA. Further, all capital and operational project expenditures must be managed in accordance with CATSA's Project Management Framework (PMF). The requirement for privacy impact analysis is embedded in the framework. If there is uncertainty as to whether a full PIA is required, employees are instructed to consult with CATSA's legal branch.

96. Based on our review of the PMF and interviews with staff engaged in the PIA process, we conclude that a formal infrastructure is in place to support the objectives and requirements of the

Treasury Board Secretariat PIA Directive. Responsibilities and accountabilities for ensuring compliance with the directive are well defined.

Process for managing privacy breaches is under development

97. The Treasury Board Secretariat's Directive on Privacy Practices requires institutions to establish a plan for addressing privacy breaches. We expected to find procedures and processes in place to meet the Treasury Board Secretariat's expectations.

98. CATSA was in the process of developing a privacy breach protocol at the time of our audit. We reviewed the draft protocol and found that it incorporates the four steps to consider when responding to a breach or suspected breach. These are: (1) breach containment and preliminary assessment; (2) evaluation of the risks associated with the breach; (3) notification; and (4) prevention.

99. A key feature of privacy management is the ability to identify, investigate and report on breaches involving personal information. The draft protocol provides a comprehensive framework for doing so.

100. RECOMMENDATION

CATSA should finalize and implement its privacy breach protocol to comply with Treasury Board Secretariat guidelines.

CATSA's response:

CATSA agrees. CATSA's draft privacy breach protocol, which is in accordance with Treasury Board guidelines for privacy breaches, was submitted to CATSA's Senior Management Committee on August 2, 2011 for review. The privacy breach protocol will be in effect by December 31, 2011.

Compliance monitoring activities need to be strengthened

101. Institutions subject to the *Privacy Act* are accountable for personal information under their control. Contracting out a program or service-delivery function does not relieve an institution from its privacy obligations under the Act or related Treasury Board Secretariat policies and directives. We expected to find that screening-service agreements addressed these obligations, and the contractors' responsibilities in that regard were clearly defined.

102. We examined the contracts between CATSA and the 11 entities that provide passenger-screening services. The confidentiality agreement that accompanied many of the initial contracts lacked key safeguards to protect passenger information. This was remedied in 2006 when CATSA amended the confidentiality agreement. We found that the revised version, which is used for all contract renewals, has a section dedicated to personal information and includes enhanced privacy protection provisions.

103. The contracts also establish CATSA's authority to audit compliance with the terms and conditions of security-screening agreements. While CATSA routinely invokes this authority for operational matters (e.g., allocation of human resources and financial management), it does not inspect or audit the personal-information handling practices of screening contractors.

104. Privacy protection extends beyond the establishment of appropriate provisions in contracting documents. A mechanism is needed to provide assurance that contractors are respecting their obligations. Periodic inspections and audits provide such a mechanism. They are also an effective tool for addressing privacy risks that can be detected only by observing the service-delivery arrangement in operation.

105. RECOMMENDATION

CATSA should ensure the management of passengers' personal information by contractors is subject to regular inspection and audit.

CATSA's response:

CATSA agrees. Audit criteria regarding the management of PI by screening contractors will be added to CATSA's airport audit program beginning the fourth quarter of fiscal year 2011–12.

Personal information is not accounted for in *Info Source*

106. The *Privacy Act* (Section 10) requires that all institutions account for and describe their personal information holdings. Descriptions of holdings are available in an index published by the Treasury Board Secretariat. This index, *Info Source*, informs the public of what personal information is held by the government, how it is managed and how to access it. Each institution is responsible for ensuring their personal information holdings are up-to-date and accurately described in the publication.

107. We reviewed the current edition of *Info Source* and found it is silent on CATSA's collection of passenger information. We also looked at CATSA's most recent submission to the Treasury Board Secretariat as part of the annual update to *Info Source*. Although the submission indicates that CATSA may accumulate categories of personal information, it cites classes of records that are stored on general-subject files (e.g., requests for information, general correspondence and enquiries). The submission does not include personal information that is stored in the Call and Incident Data Collection System (e.g., security incident and complaint records) or personal information that is captured by the various technologies used to monitor and screen passengers.

Exhibit 2: Example of closed-circuit television sign near screening queue

108. In addition, at the time of our audit, we found a lack of transparency regarding the use of closed-circuit television in passenger screening areas. Only four of the eight airports we visited had signage that was visible to passengers upon entry to the screening queue. Moreover, the signage states that area may be monitored. We confirmed that the cameras continuously record passenger movement and video footage is retained for a minimum of 30 days.

109. We also observed that passengers were not always informed of their options when subjected to a physical search. CATSA uses technology to randomly select individuals for additional (secondary) screening. When referred for additional screening, a passenger has the option of a full-body image scan, a physical pat-down in public view, or a physical pat-down in a private search area (a partitioned stall or room). We observed the secondary screening process at five airports. Passengers were typically asked

to choose between a full-body scan and a pat-down in public view; we observed that the option of a physical pat-down in a private search area was rarely offered. Given the intrusive nature of secondary screening, it is important that passengers possess the knowledge necessary to make an informed decision.

110. RECOMMENDATION

To satisfy its obligations under the *Privacy Act,* CATSA should ensure that all categories of personal information under its control are listed and described in the next edition of *Info Source*. Further, in a spirit of openness and transparency, CATSA should also ensure that passengers are:

- aware that closed-circuit television is used to monitor and record their movement through the screening process; and
- informed of the three physical search options upon referral to secondary screening.

CATSA's response:

CATSA agrees. CATSA will continue to work collaboratively with Treasury Board Secretariat to ensure the personal information under its control is listed and described in the 2011 edition of *Info Source*.

There are currently 31 airports in Canada that have CCTV. CATSA is in the process of providing updated signs to all 31 airports to ensure passengers are aware that CCTV is used to monitor and record their movement through the screening process. The updated CCTV signage wording states: "This area is monitored by video camera," thereby eliminating any conditional language and ambiguity for the passenger. The task will be completed by October 1, 2011.

It is CATSA's policy to inform passengers about the options for private search when selected for secondary screening. Screening officers are trained to offer the options, signage is on display, details are available on CATSA's website, and the Operations Performance Oversight Program reviews compliance. Screening officers will be reminded through shift briefings of the requirement to inform passengers of the physical search options upon referral for secondary screening.

Privacy awareness is not part of the core training program

111. Compliance with the spirit and requirements of the *Privacy Act* depends largely on how well it is understood by those handling personal information. Awareness and training are essential to achieve the Act's objectives. We expected to find a comprehensive privacy component in CATSA's training program. We reviewed course materials and interviewed the director responsible for staff awareness initiatives.

112. We were informed that privacy awareness training has not been delivered to employees at CATSA's head office. In terms of front-line officers, the course curriculum focuses on passenger-screening processes. Officers are supplied with various reference sources for this purpose, with CATSA's standard operating procedures (SOPs) being central in this regard. The SOPs cover all aspects of passenger and baggage screening and provide information on the testing and operation of screening technologies. The SOPs also highlight the importance of handling records with proper care and the consequences of an unauthorized disclosure of confidential information. While these are noteworthy, the SOPs are deficient in terms of addressing other core privacy principles in significant detail, such as the safeguarding and disposal of passengers' personal information.

113. We also made inquiries to ascertain whether CATSA had a corporate privacy policy and found that it did not. Such an instrument would provide a means of establishing clear accountability for privacy compliance and would ensure that all employees and contract staff possess an understanding of their roles and responsibilities in meeting the obligations established under the *Privacy Act*.

114. RECOMMENDATION

CATSA should expand current training initiatives to ensure that all employees and contract screening officers who handle personal information possess a sound knowledge of core privacy principles.

CATSA's response:

CATSA agrees. Privacy principles that are articulated in the Standard Operating Procedures will be incorporated into training material for front-line personnel where required. Subsequent to the approval of a corporate privacy policy and breach protocol, CATSA will ensure that all contract staff and their employees understand and comply with these requirements. Training will be developed during 2011–12 to be delivered to all employees and the screening workforce in 2012–13.

Conclusion

115. The *Privacy Act* imposes obligations on federal institutions to respect the privacy rights of Canadians by placing limits on the collection, use and disclosure of personal information.

116. Within the federal context, the collection of personal information must be relevant to an operating program or activity of the federal institution. Relevance is determined by statutory authority. Some of CATSA's collection activities are for general law enforcement investigative purposes. These are unrelated to CATSA's aviation security mandate and therefore beyond its statutory authority. In addition, CATSA has not demonstrated that the collection of personal information is necessary to validate the authenticity of boarding passes, or that the loss of privacy resulting from the collection is proportionate to the need. CATSA should establish mechanisms to ensure its personal information holdings are both relevant and not excessive.

117. Although its use and disclosure practices generally comply with the *Privacy Act*, we found that CATSA notifies the police when large sums of money are discovered on or in the baggage of domestic travellers. Such disclosures do not respect privacy. It is not an offence to travel with a large sum of money, nor does it constitute a threat to aviation security. It would rarely, if ever, be apparent to CATSA screening officers that the money may constitute evidence of a crime. Additional investigation would be required to make such a determination, something that exceeds both CATSA's expertise and mandate.

118. A number of technologies have been introduced to facilitate passenger screening, including full-body image scanners. While the security framework surrounding full-body imaging technology is sound, procedures designed to protect privacy are not consistently followed. This could place scanned images—and potentially the identity of the passenger—at risk of exposure.

119. Government institutions are responsible for implementing adequate physical, technical and administrative controls to protect personal information. We found no evidence that passenger information could be compromised because of inadequate safeguards at CATSA's head office. However, we did observe deficient storage and disposal practices at some airports.

120. CATSA has outsourced passenger screening to 11 private sector companies. It does not systematically inspect or audit contractors' handling of passenger information. CATSA has been guided by the assumption that screening contractors are managing the information appropriately without any assurance that this is so. This gap needs to be addressed. In the absence of an effective monitoring regime, contractors may circumvent their privacy obligations without consequence.

121. Based on our audit work, we concluded that CATSA is not fully complying with the *Privacy Act*. Addressing the findings in this report will assist CATSA in meeting its aviation security objectives while respecting the privacy rights of air travellers.

About the Audit

AUTHORITY

Section 37 of the *Privacy Act* empowers the Privacy Commissioner to examine the personal-information handling practices of federal government organizations.

OBJECTIVE

The audit objective was to assess whether the Canadian Air Transport Security Authority (CATSA) has implemented adequate controls to protect passengers' personal information, and whether its policies, procedures and processes for managing such information comply with the fair information practices embodied in sections 4 through 8 of the *Privacy Act*.

CRITERIA

Audit criteria are derived from the *Privacy Act* and Treasury Board Secretariat policies, directives and standards directives related to the management of personal information.

We expected to find that CATSA:

- limits the collection and use of personal information to that which is necessary for the execution of its aviation security mandate;
- restricts the disclosure of personal information to that which is authorized by law;
- retains and disposes of personal information in accordance with governing authorities;
- protects personal information throughout its life cycle; and
- has implemented a framework to satisfy its obligations under the *Privacy Act*.

SCOPE AND APPROACH

Audit evidence was obtained through various means, generally involving on-site examinations, interviews and information obtained through correspondence. We also reviewed policies, procedures, supporting systems and an exploratory sample of security incident reports. Control testing was performed on full-body scanning technology at selected airports and at CATSA's testing facility.

Audit activities were carried out in the National Capital Region and at eight airports. The audit work was substantially completed on March 31, 2011.

STANDARDS

The audit was conducted in accordance with the legislative mandate, policies and practices of the Office of the Privacy Commissioner of Canada, and followed the spirit of the audit standards recommended by the Canadian Institute of Chartered Accountants.

AUDIT TEAM

Director General: Steven Morgan

Dan Bourgeault
Gaetan Letourneau
Loren Myers
Anne Overton
Bill Wilson

Appendix A: List of Recommendations

COMPLIANCE WITH CODE OF FAIR INFORMATION PRACTICES

RECOMMENDATION

CATSA should implement measures to ensure the collection of personal information is limited to aviation security incidents.

CATSA's response:

CATSA agrees to implement measures to ensure the collection of personal information is limited to aviation security incidents.

With respect to situations involving Explosive Detection Trace (EDT) alarms, CATSA is required by the Security Screening Order (SSO) to keep a record of every instance in which this alarm is triggered. CATSA will consult with Transport Canada to confirm what types of information are necessary to meet the reporting requirements of the SSO.

RECOMMENDATION

CATSA should more clearly inform passengers of the purposes for which BPSS data is collected, the uses that are made of it, to whom and under what circumstances the information may be shared with third parties, and how long the data is kept.

CATSA's response:

CATSA agrees and will ensure that passengers are properly informed of the purposes for which BPSS data is collected, the retention period and potential disclosures. This information will be included in a new privacy notice to be distributed by December 1, 2011 at locations where BPSS is deployed. CATSA will also continue to work collaboratively with the Treasury Board Secretariat to ensure that BPSS information is accurately described in the next edition of *Info Source*.

RECOMMENDATION

CATSA should:

- cease the practice of notifying police when it discovers a large sum of money in the baggage of or on an individual travelling domestically; and
- ensure that all disclosures to airline carriers are limited to only that which is necessary in the circumstances of each case.

CATSA's response:

CATSA agrees and will implement the recommendation. Amendments to CATSA's Standard Operating Procedures (SOPs) will be included in the next release, scheduled for early in the third quarter of 2011–12.

RECOMMENDATIONS

CATSA should permanently delete all personal information held in its information holdings (electronic and hard copy records) that it does not have the authority to collect, specifically records capturing the fortuitous discovery of:

- contraband, including illegal narcotics;
- items that are initially perceived to pose a threat to aviation security and the threat is determined to be non-existent after further examination and/or police intervention;
- items that appeared to be illegal and required investigation beyond CATSA's mandate and expertise; and
- large sums of money carried by or in baggage of passengers.

CATSA should also consult with Library and Archives Canada to establish a records retention and disposal schedule for personal information collected under its aviation security mandate.

CATSA's response:

CATSA agrees and will implement these recommendations. An action plan will be developed.

SAFEGUARDING PASSENGERS' PERSONAL INFORMATION

RECOMMENDATION

Given the privacy concerns surrounding the use of full-body scanning technology, CATSA should:

- ensure that procedural safeguards to protect privacy are understood, enforced and subject to ongoing compliance monitoring; and
- conduct a physical inspection of all full-body scan viewing rooms and disable any closed-circuit television installations.

CATSA's response:

CATSA agrees. As a result of an earlier consultation with the Office of the Privacy Commissioner of Canada, privacy safeguards were put in place. CATSA will continue to ensure that established safeguards are understood and adhered to by all employees, screening contractors and screening officers. CATSA will issue a shift briefing to remind screening personnel of the established SOPs for full-body scanners. Additionally, CATSA will inspect all full-body scanner deployments to ensure that all privacy safeguards are respected. Both activities will be completed in the third quarter of 2011–12.

The observation regarding the CCTV camera was an isolated incident and has been corrected.

RECOMMENDATION

CATSA should subject the Call and Incident Data Collection (CIDC) System to a formal certification and accreditation process.

CATSA's response:

CATSA agrees. The CIDC system has been replaced by a new system called the Service Monitoring and Recording Toll (SMART). CATSA will be certifying and accrediting the new system in-house. The accreditation authority for SMART will be the Program/Service Delivery Manager.

RECOMMENDATION

To meet Treasury Board Secretariat requirements and ensure passenger information is adequately protected, CATSA should apply a security designation that is commensurate with the sensitivity of the information. It should also ensure that:

- the designation is marked on the information and is reflected in CATSA's standard operating procedures; and
- screening contractors implement physical security measures that comply with Treasury Board Secretariat standards.

CATSA's response:

CATSA agrees. In July 2011, CATSA issued a new directive (Directive #56) to all screening contractors. This directive highlights the importance of handling information properly; provides guidance about the types of information that require special handling that they are most likely to see;

and indicates how to store, transmit and destroy documents containing these types of information. A further update to this directive will be provided to screening contractors as a reminder to follow the retention periods listed on the forms where PI is collected.

Audit criteria regarding the management of passenger PI by screening contractors will be added to CATSA's airport audit program in the fourth quarter of fiscal year 2011–12.

RECOMMENDATION

CATSA should:

- ensure that all contracts related to the disposal of personal information collected under its legislative mandate comply with Treasury Board Secretariat requirements;
- implement a protocol for monitoring off-site destruction practices; and
- ensure off-site destruction contracts include a requirement that the service provider issue a certificate of destruction recording the date records are destroyed and the name of the authorized officer who conducted or witnessed the destruction.

CATSA's response:

CATSA agrees. Provisions governing the proper disposal and off-site destruction of passenger PI will be written into the new airport screening-services agreements to be implemented as of November 1, 2011.

In addition, as noted in CATSA's response to the preceding recommendation, in July 2011, CATSA issued a new directive (Directive #56) to all screening contractors. The directive highlights the importance of handling information properly; provides guidance to screening contractors about the types of information requiring special handling that they are most likely to see; and indicates how to store, transmit and destroy documents containing these types of information.

Audit criteria regarding the management of passenger PI by screening contractors will be added to CATSA's airport audit program beginning in the fourth quarter of 2011–12.

PRIVACY LEADERSHIP AND ACCOUNTABILITY

RECOMMENDATION

CATSA should finalize and implement its privacy breach protocol to comply with Treasury Board Secretariat guidelines.

CATSA's response:

CATSA agrees. CATSA's draft privacy breach protocol, which is in accordance with Treasury Board guidelines for privacy breaches, was submitted to CATSA's Senior Management Committee on August 2, 2011 for review. The privacy breach protocol will be in effect by December 31, 2011.

RECOMMENDATION

CATSA should ensure the management of passengers' personal information by contractors is subject to regular inspection and audit.

CATSA's response:

CATSA agrees. Audit criteria regarding regarding the management of PI by screening contractors will be added to CATSA's airport audit program beginning the fourth quarter of fiscal year 2011–12.

RECOMMENDATION

To satisfy its obligations under the *Privacy Act*, CATSA should ensure that all categories of personal information under its control are listed and described in the next edition of *Info Source*.

Further, in a spirit of openness and transparency, CATSA should also ensure that passengers are:

- aware that closed-circuit television is used to monitor and record their movement through the screening process; and
- informed of the three physical search options upon referral to secondary screening.

CATSA's response:

CATSA agrees. CATSA will continue to work collaboratively with Treasury Board Secretariat to ensure the personal information under its control is listed and described in the 2011 edition of *Info Source*.

There are currently 31 airports in Canada that have CCTV. CATSA is in the process of providing updated signs to all 31 airports to ensure passengers are aware that CCTV is used to monitor and record their movement through the screening process.

The updated CCTV signage wording states: "This area is monitored by video camera," thereby eliminating any conditional language and ambiguity for the passenger. The task will be completed by October 1, 2011.

It is CATSA's policy to inform passengers about the options for private search when selected for secondary screening. Screening officers are trained to offer the options, signage is on display, details are available on CATSA's website, and the Operations Performance Oversight Program reviews compliance. Screening officers will be reminded through shift briefings of the requirement to inform passengers of the physical search options upon referral for secondary screening.

RECOMMENDATION

CATSA should expand current training initiatives to ensure that all employees and contract screening officers who handle personal information possess a sound knowledge of core privacy principles.

CATSA's response:

CATSA agrees. Privacy principles that are articulated in the Standard Operating Procedures will be incorporated into training material for front-line personnel where required. Subsequent to the approval of a corporate privacy policy and breach protocol, CATSA will ensure that all contract staff and their employees understand and comply with these requirements. Training will be developed during 2011–12 to be delivered to all employees and the screening workforce in 2012–13.

Appendix B: List of Prohibited Items

PROHIBITED ITEMS FOR PASSENGERS ON ALL FLIGHTS

Guns, firearms and other devices designed to cause serious injury by launching harmful objects or items that could be mistaken for such a device, including:

- firearms of all types, including pistols, revolvers, rifles, shotguns
- toy, replica and imitation weapons that could be mistaken for real weapons
- parts of firearms (excluding telescopic sights)
- compressed air and CO_2 guns, including pistols, pellet guns, rifles and ball bearing guns
- signal flare pistols and starter pistols
- bows, crossbows and arrows
- harpoon guns and spear guns
- slingshots and catapults

Devices designed to stun or immobilize, including:

- devices for shocking, such as stun guns (e.g., tasers) and stun batons
- animal stunners
- chemicals, gases and sprays such as mace, pepper spray or capsicum spray, tear gas, acid sprays and animal repellent sprays

Objects with sharp points or sharp edges that could be used to cause serious injury, including:

- items designed for chopping, such as axes, hatchets and cleavers
- ice axes and ice picks
- razor-type blades such as box cutters, utility knives and safety razor blades
- knives or knife-like objects of any length
- scissors with blades longer than 6 cm as measured from the fulcrum
- martial arts equipment with sharp points or sharp edges
- swords, sabres

Work tools that could be used to either cause serious injury or threaten the safety of aircraft, including:

- crowbars, hammers
- drills and drill bits, including cordless portable power drills
- tools with shafts longer than 6 cm (excluding the handle) that could be used as weapons, such as screwdrivers and chisels
- saws, including cordless portable power saws
- blowtorches, gas torches
- bolt guns and nail guns

Blunt objects that could be used to cause serious injury when used to hit, including:

- sporting bats
- golf clubs, billiard cues, ski poles
- hockey sticks, lacrosse sticks
- brass knuckles
- clubs and batons, such as billy clubs, blackjacks and night sticks
- martial arts weapons

Explosive or incendiary substances or devices that could be used to cause serious injury or threaten the safety of the aircraft, including:

- ammunition, propellant powder, gunpowder
- blasting caps
- detonators and fuses
- replica or imitation explosive devices
- mines, grenades and other military supplies
- flares or fireworks
- canisters or cartridges that create smoke

Liquids, aerosols and gels:

- liquids, aerosols or gels—other than formula, milk, breast milk, juice or food for infants—in containers that exceed 100 ml or 100 g in capacity and that do not all fit in a single clear plastic resealable bag that is sealed and does not exceed 1 L in capacity

Dangerous goods:

- dangerous goods as defined in section 2 of the *Transportation of Dangerous Goods Act, 1992* that are not being transported as set out in part 12 of the Transportation of Dangerous Goods Regulations
- caustic materials (including acids)
- carbon dioxide cartridges and other compressed gases

Source: Transport Canada website (www.tc.gc.ca/eng/aviationsecurity/page-147.htm)