

Passenger Protect Program Transport Canada

Section 37 of the Privacy Act



Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

2009



Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

AUDIT OF PASSENGER PROTECT PROGRAM, TRANSPORT CANADA

The audit work reported here was conducted in accordance with the legislative mandate, policies, and practices of the Office of the Privacy Commissioner of Canada.

This report is available on our Web site at www.priv.gc.ca.

For copies of reports or other Office of the Privacy Commissioner publications, contact:

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

Telephone: (613) 995-8210, or 1-800-282-1376
Fax: (613) 947-8210
E-mail: publications@priv.gc.ca

Table of Contents

- Main Points** 1
- Introduction** 2
- Observations and Recommendations** 5
 - Transport Canada has adequate collection controls to protect personal information. 5
 - Transport Canada has acceptable controls for the use of personal information. 6
 - Transport Canada has controls for the retention of personal information. 7
 - Mechanisms exist to ensure that the Specified Persons List is accurate. 7
 - The Deputy Minister does not obtain complete information for Specified Persons List decision making. 9
 - Transport Canada has physical measures, training programs and security clearances to safeguard personal information held within the Passenger Protect Program. 9
 - Transport Canada can not demonstrate that the Specified Persons List information technology application has been certified and accredited to meet the requirements of government security standards. 10
 - There is no requirement for airlines to report data breaches. 12
 - Transport Canada has not verified that airlines are adequately protecting personal information. 12
- Conclusion** 13
- About the Audit** 14

Main Points

What we examined

Our audit examined whether Transport Canada (the Department) has adequate controls and safeguards to collect, use, disclose, retain, dispose, protect and ensure the accuracy of personal information under the Passenger Protect Program. The core of the Passenger Protect Program is the Specified Persons List, otherwise known as Canada's "No-fly list".

What we found

Transport Canada collects and uses personal information within the Passenger Protect Program in accordance with the *Privacy Act* and the *Aeronautics Act*.

The Deputy Minister at Transport Canada was not provided with complete information when deciding to add or remove names to or from the Specified Persons List. This situation may raise questions about the decision-making process if an incomplete record were to result in an incorrect change to the Specified Persons List.

Transport Canada generally uses adequate physical measures, training programs and security clearances to safeguard personal information within the Passenger Protect Program. However Transport Canada has not demonstrated that the Specified Persons List application used to disclose Specified Persons List information to air carriers has been certified and accredited to meet Government Security standards. An information technology system that has not been certified and accredited increases the likelihood of undetected security weaknesses, which could render sensitive personal information vulnerable within the Passenger Protect Program.

Currently there are no requirements that air carriers report security breaches involving personal information to Transport Canada.

Transport Canada has not yet extended its oversight activities to verify that airlines are aware of and complying with all requirements of the Identity Screening Regulations related to the handling and safeguarding of Specified Persons List information disclosed by the department. There is a further risk that the Specified Persons List information could be inappropriately disclosed due to two air carriers which rely on a paper copy of the list.

Why it is important

The Passenger Protect Program involves very sensitive personal information that identifies individuals who Transport Canada considers as representing an immediate threat to aviation security.

The decisions to place someone on the Specified Persons List and to subsequently refuse that person permission to board an aircraft are serious ones. A decision to deny boarding could have a negative impact on the individual's reputation and his or her work opportunities and ability to travel in the future.

This audit is intended to assess the adequacy of Transport Canada's practices for the handling and safeguarding of personal information within the Passenger Protect Program.

Introduction

1. While aviation security has always been a priority for governments and airlines, the terrorist events of September 11, 2001 were the catalyst for more and expanded aviation security measures around the world. Canada was not an exception. The Canadian government has created a number of national security programs affecting the privacy of Canadians. Some new programs introduced over the past decade have included: the Advanced Passenger Information program, which obliges air carriers to collect detailed passenger information; the introduction of new passenger screening measures; and the creation of trusted traveller programs such as NEXUS.
2. Many national security programs involve the collection of personal information about large numbers of travellers with the intent of stopping a small number of terrorists or criminals. Some of these measures have also resulted in the creation of lists of passengers considered to be of high risk. These flagged individuals may be subjected to more intensive screening and/or other travel restrictions.
3. The Passenger Protect Program (the Program) is a passenger screening program which was implemented on June 18, 2007. The legal authority for the Program is the *Aeronautics Act* as amended in 2004.
4. Transport Canada's declared goal for the Program is to improve aviation security by reducing the threat of terrorism and other criminal acts on flights to or from Canada. "Aviation Security" under the *Aeronautics Act* also applies to aircraft, airports, aviation facilities, and the safety of the public, passengers and crew members.
5. The Specified Persons List (the List) is used as a screening tool by domestic and foreign air carriers and Transport Canada to prevent persons named on the list from boarding any domestic flights or international flights leaving or bound for Canada at airports designated in the Canadian Air Transport Security Authority Aerodrome Designation Regulations.
6. Transport Canada's Identity Screening Regulations as amended in 2008 set out the procedures for air carriers to screen passengers on behalf of Transport Canada for the Passenger Protect Program and their obligations to safeguard this information.
7. The Passenger Protect Program is a secretive program, with Transport Canada adding names of individuals to the List without those individuals' knowledge. The Program also involves both the collection and the disclosure of sensitive personal information from and to the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS) without individuals' knowledge or consent.
8. From 2005 to 2006, the Office of the Privacy Commissioner of Canada (OPC) reviewed two Privacy Impact Assessments about the Program, one received from Transport Canada and the other from the Department of Public Safety and Emergency Preparedness Canada on behalf of CSIS and the RCMP.

The Office of the Privacy Commissioner made several recommendations to these departments at that time to eliminate and mitigate some of the most serious privacy impacts of the Program. Transport Canada, CSIS and the RCMP implemented many of the Commission's recommendations soon after.

9. Some of those changes implemented by Transport Canada included:

- creation of Identity Screening Regulations to create enforceable standards for air carriers' handling and protection of personal information;
- increase of the minimal age for passenger screening from 12 years of age to 18;
- establishment of personal information retention schedules and InfoSource listings for Passenger Protect Program information;
- implementation of Standard Operating Procedures for the Office of Reconsideration and for Transport Canada Intelligence Duty Officers.
- recording details of calls from air carriers about the Specified Persons List, including any positive or negative matches; and
- communication of a summary of the Privacy Impact Assessment and responses to Privacy Commission's questions about the Program on the Transport Canada website to inform the public.

How the Program works

10. The Passenger Protect Program is a centralized program situated at Transport Canada's headquarters in Ottawa and employs approximately 20 people. Other Transport Canada employees in Information Technology and in Aviation Security Operations also support the Program. The cost of implementing the Program was estimated by Transport Canada in 2007 at \$13.8 million over the first five years, and \$2.9 million per year after that.

11. Under the Program, the airlines screen travellers against Transport Canada's Specified Persons List, which consists of names of people whom Transport Canada believes may pose an immediate threat to aviation security if they were to board an aircraft.

12. Transport Canada creates the List based on information provided by the RCMP and CSIS. Senior representatives of Transport Canada, CSIS and the RCMP form the Specified Persons List Advisory Group (Advisory Group). The Advisory Group meets on a regular basis to review the existing List, to share information about potential candidates for the List and to recommend names to be added to or removed from the List to the Deputy Minister at Transport Canada.

13. Paragraph 4.81(1) of the *Aeronautics Act* indicates that "the Minister or any other officer of the Department of Transport authorized by the Minister..." may require information from any air carrier concerning "any particular person specified by the Minister or officer." This is the only reference in the *Aeronautics Act* to specified persons. It is a collection of these persons' names which constitutes the Specified Persons List used by air carriers and Transport Canada for passenger screening purposes.

14. In the files we examined, it is the Deputy Minister at Transport Canada who makes the final decision about inclusions and deletions to the Specified Persons List.

15. According to the Identity Screening Regulations, airlines must verify all passenger names against the List at check-in. If the passenger's name matches a name on the List, airlines officials will then ask the passenger for identity information, such as a passport, that includes their name, date of birth and gender. Transport Canada advised us that most air carriers use an automated system to check passenger identity information against Specified Persons List information. For all but two smaller airlines subject to the Program, where there is a match between the passenger's information and the List, the airline agent receives an electronic flag on the reservation system. This flag advises the agent to contact their security office for further instructions.

16. Access to the actual listed information is limited to a small number of airline security officials and is not accessible to front line airline staff except for the two airlines as referred to above. If a match is confirmed by the airline's security official between a passenger's name, date of birth and gender with the same information on the List, a designated airline official must immediately notify Transport Canada's Intelligence Operations and Support Centre by telephone.

17. Once advised of a match by the airlines, the Department carries out its own verification to confirm whether the passenger identified by the airlines is actually the person on the List. The Department uses additional passenger information obtained from the airlines to compare with information in the Department's own more detailed Specified Persons List files. Paragraph 4.81(1) of the *Aeronautics Act* allows Transport Canada to collect additional personal information from the air carriers about specified persons.

18. Some examples of the 34 elements of personal information listed in the Act include the passenger's name, date of birth, gender, address, citizenship; passport, visa and ticket numbers, itinerary, destination, seat assignment and baggage information.

19. If a positive match has been determined by the Transport Canada officer, the officer makes the decision to deny or allow boarding.

20. When an individual is denied boarding under subsection 4.76 of the *Aeronautics Act*, the Department immediately issues the individual with an official notice. This Emergency Direction provides the reason for the denial of boarding and indicates that the individual has the right to submit an application of reconsideration to Transport Canada. The purpose of the reconsideration process is to review the Deputy Minister's decision to have included the individual on the List.

21. The application of reconsideration places the onus on the individual to provide the grounds for reconsideration. The individual must also sign a consent allowing Transport Canada to disclose the individual's personal information to CSIS, the RCMP, law enforcement agencies and/or to Citizenship and Immigration Canada "for the purposes of verifying the accuracy of the information provided".

22. The Office of Reconsideration at Transport Canada engages security advisors on a contractual basis to review applications for reconsideration and to make recommendations to the Deputy Minister about whether the person should have been named on the List or not.

23. Individuals may also apply to the Federal Court of Canada for a judicial review of Transport Canada's decision. One such application has been filed with the Court to date.

Focus of the Audit

24. The focus of the audit was to determine whether Transport Canada has adequate controls and safeguards to collect, use, disclose, retain, dispose, protect and ensure the accuracy of personal information under the Passenger Protect Program.

25. The audit did not examine the effectiveness of the program, nor did it examine the reliability of information used to determine whether specific individuals should have been added to the Specified Persons List or not as these two questions fall outside the mandate of the OPC. Finally, the audit did not examine the personal information handling practices of airlines, although we did examine Transport Canada's oversight role in this regard.

26. It is important to note that a passenger destined for or leaving Canada may be denied boarding to an aircraft based on information other than Transport Canada's Specified Persons List. The United States No-Fly list and the United Nations list of terrorists are two lists that are used to screen passengers and may result in a decision to deny boarding to named individuals. A Canadian citizen, Abousfian Abdelrazik, for instance, was stranded in Sudan and unable to return to Canada for a number of years because of his inclusion on the United Nations list of terrorists. These other lists are outside the Privacy Commissioner's mandate.

Observations and Recommendations

27. To assess Transport Canada's privacy practices against our various audit criteria we conducted interviews with Program officials in several program areas, observed processes where possible and conducted site visits of facilities. We also reviewed documentation such as data-flow diagrams and descriptions, standard operating procedures, agreements between partners, terms of reference and minutes of meetings for the Advisory Group, training materials, forms, incident reports of the Intelligence Operations and Support Section, retention schedules and procedures and operational files from the Office of Reconsideration.

Transport Canada has adequate collection controls to protect personal information.

28. Sections 4 and 5 of the *Privacy Act* govern the collection of personal information. Section 4 indicates that any personal information collected by a federal government department or agency must relate directly to the programs or activities of the institution. With certain exceptions, section 5 requires institutions to collect personal information directly from the person concerned and that the person is informed of the purpose of the collection.

29. For the purposes of our audit, we therefore expected that Transport Canada would only collect personal information for the purposes of the Passenger Protect Program and its activities under section 4 of the *Privacy Act*. We also expected Transport Canada to inform the person concerned of the purposes of the collection unless permitted otherwise under the exceptions at paragraph 5(3)(b) of the *Privacy Act*.

30. Finally, we expected that Transport Canada had controls in place to ensure the proper collection of personal information in compliance with the above provisions.

31. We found that the information collected by Transport Canada relates to the Program and its activities. We found also that Transport Canada collects personal information directly from travellers, providing the reason for collection and obtaining their consent when this is possible—for example, information obtained from individuals to support an Application for Reconsideration.

32. Where Transport Canada collects personal information from the airlines, CSIS and the RCMP, this is done without the knowledge or consent of the individual to whom the information relates. However, these specific non-consensual collection activities are permitted under the exceptions found at section 5(3) of the *Privacy Act*. As this information relates to individuals who may be a threat to aviation security, to advise these individuals of the collection “might defeat the purpose, or prejudice the use for which the information was collected”, as stated in paragraph 5(3)(b) of the *Privacy Act*.

33. We also found that Transport Canada has standard operating procedures, agreements with partners and standard forms in place to ensure that it collects only the personal information that it needs to administer the Program.

Transport Canada has acceptable controls for the use of personal information.

34. The use and disclosure of personal information is governed by sections 7 and 8 of the *Privacy Act*. In general terms, these sections allow government departments and agencies to use and disclose personal information with the individual’s consent and only for the purposes for which they have collected it, as part of the operation of their programs and activities.

35. Sections 7 and 8 of the *Privacy Act* do contain a number of exceptions allowing personal information to be used or disclosed without the individual’s consent. An example of a permissible disclosure without consent is found at paragraph 8(2)(b) of the *Privacy Act* “for any purpose in accordance with an Act of Parliament or any regulation made thereunder...” (such as paragraph 4.81(3) of the *Aeronautics Act* allowing Transport Canada to disclose Passenger Protect Program information to CSIS and the RCMP).

36. We expected that Transport Canada’s use and disclosure activities within the Program would be in compliance with the requirements of sections 7 and 8 of the *Privacy Act*. We also expected to find that the Department would have adequate controls in place to ensure the proper use and disclosure of personal information.

37. We found that the Department discloses personal information selectively to officials who have a need to use information to carry out the Program. It also limits the disclosure of personal information to that information which is essential to operating the Program. Within each of the Program's administrative units, the use and disclosure of personal information is limited to a small number of officials.

38. While most of Transport Canada's disclosure practices were found to be adequate, one exception would be for Specified Persons List information disclosed to air carriers. As noted later in the report, we question Transport Canada's lack of oversight activities to verify that airlines are properly handling and protecting Specified Persons List information obtained from the Department. This is even more of a concern for two smaller airlines, which print copies of the List that may go astray.

Transport Canada has controls for the retention of personal information.

39. Retention and disposal of personal information is subject to subsections 6(1) and 6(3) of the *Privacy Act*. Subsection 6(1) provides for the retention of personal information used for administrative purpose for a period prescribed by regulations. The *Privacy Act Regulations* prescribe a minimum retention period of two years. Subsection 6(3) requires that personal information be disposed of in accordance with regulations, directives and guidelines for that information.

40. We note that the disposal of personal information is also subject to the requirements of sections 12 and 13 of the *Library and Archives Act*. These provisions require that organizations have a Records Disposition authority approved by the National Archivist for all of its program records.

41. We expected Transport Canada to comply with subsections 6(1) and (3) of the *Privacy Act* and to have controls for the proper retention and disposal of personal information

42. Transport Canada retains personal information according to the departmental retention schedule of which we found Transport Canada employees were aware. The retention period of five years for various types of information relating to the Passenger Protect Program is appropriate to the Program's requirements and with the requirements of subsection 6(1) of the *Privacy Act*. As the Program is relatively new, most records had not yet attained their period of five years of retention before these records would be sent to Library and Archives and we were therefore unable to verify if this retention schedule was followed by Transport Canada.

Mechanisms exist to ensure that the Specified Persons List is accurate.

43. Subsection 6(2) of the *Privacy Act* underscores the department's obligations to take reasonable steps to ensure that the personal information used for administrative purposes is as accurate, up-to-date and complete as possible. Section 3 of the *Privacy Act* defines "administrative purpose" as "the use of ...information in a decision making process that directly affects that individual."

44. The quality of Passenger Protect Program information is essential to ensure that a decision to add or remove a person's name to or from the Specified Persons List is well founded. Sound information is also essential for establishing a valid positive match between a name on the List and a passenger whom an airline has identified as possibly being on that List.

45. We expected to find that Transport Canada was complying with the requirements of subsection 6(2) of the *Privacy Act* that personal information used for an administrative decision be as accurate, up-to-date and complete as possible.

46. We also expected that Transport Canada would have controls to ensure that information was accurate, up-to-date and complete.

47. In interviewing Transport Canada staff, reviewing files relating to the Specified Persons List, and examining incident reports and notes from the Advisory Group meetings, we found no evidence that the information which Transport Canada collected, used or disclosed was inaccurate. Transport Canada receives personal information for nominations of specified persons from the RCMP and CSIS, and relies on these organizations to ensure that information provided is accurate, complete and up to date.

48. Transport Canada uses various controls in agreements and Terms of References with CSIS and the RCMP to ensure the quality of the information related to the Passenger Protect Program. These agreements and Terms of References provide opportunities for CSIS, the RCMP and Transport Canada officials and their Advisory Group representatives to challenge the accuracy of any information about current or proposed specified persons. There is also a requirement in the Terms of Reference for CSIS and the RCMP to review Specified Persons List nominations every 30 days. The Terms of Reference also indicates that any errors or necessary modifications to listed information are to be raised with the Advisory Group as soon as possible for correction.

49. By using multiple data elements to determine if a positive match exists between Specified Persons List and passenger information, Transport Canada may limit the chances of errors in matching (i.e. false positives) and also reduce the risk that a traveller will be falsely identified and be denied boarding to an aircraft.

50. A 'false positive' in the context of the Program would be where a legitimate traveller is mistakenly matched to the List. Causes for false positives could include human error and/or the use of inaccurate information.

51. When an airline employee identifies a traveller as being someone who may be on the List, Transport Canada must reconfirm if there is a positive match by comparing selected personal information from the Specified Persons List files with additional passenger information obtained from the airlines. For instance, Transport Canada may verify whether there is a match of a passport number from the Specified Persons List file with the passport number held by an air carrier in their ticket reservation system. One or more elements of passenger information may be verified by Transport Canada until a positive match or negative match has been determined.

The Deputy Minister does not obtain complete information for Specified Persons List decision making.

52. It is the Deputy Minister at Transport Canada who makes decisions about the addition or deletion of names to or from the Specified Persons List. These decisions are made based on the advice and information provided by the Advisory Group.

53. While the audit did not find problems with the accuracy of Passenger Protect Program information at Transport Canada, we found that the Advisory Group does not provide information to the Deputy Minister that is as complete as the information which it reviews in arriving at its recommendations. In this regard, the Deputy Minister does not receive a copy of the records, meeting notes and full reasons supporting the Advisory Group's recommendations.

54. The purpose of providing a complete record to a delegated official making an important administrative decision is to ensure that the decision maker has sufficient information to review and to make up their own mind, whether the evidence supports the recommendation or not.

55. Transport Canada's procedure of providing a less than complete record to the Deputy Minister could have serious consequences to the livelihood, reputation and ability to travel of the person named.

Recommendation: The Deputy Minister or other delegated official authorized to decide whether to add or remove names of persons to or from the Specified Persons List should be provided with sufficient information from the Specified Persons List Advisory Group before a final decision is made.

Transport Canada's management response:

"Transport Canada agrees with this recommendation. Although procedural changes were implemented in February of 2009 (at the time of the audit) to ensure that the decision maker receives all necessary information to make an informed decision, no recommendations from the Specified Persons List Advisory Group (SPLAG) to the Deputy Minister to add or remove an individual to the Specified Persons List were made under this new process until after the examination phase of the audit."

Transport Canada has physical measures, training programs and security clearances to safeguard personal information held within the Passenger Protect Program.

56. The purpose of the *Privacy Act* as set out at section 2 is to "extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information."

57. The *Privacy Act* does not contain any more specific provisions about the safeguarding of personal information. However, Treasury Board Secretariat has created a number of policies for the protection of information including personal information within the federal government. These include the Government Security Policy, the Policy for the Management of Government Information as well as other more specific security related requirements. Although the Government Security Policy was replaced by the Policy on Government Security

on July 1, 2009, it was the Government Security Policy that was effective during the course of our audit.

58. We expected that Transport Canada would comply with the Government Security Policy and related policies, standards and other guidelines.

59. Our audit focused primarily on physical, administrative, personnel and Information Technology security. For physical security we conducted site visits to assess the adequacy of various controls such as security guards, restricted access zones and approved storage containers according to the Treasury Board Operational Security Standard on Physical Security.

60. For administrative security, we examined whether Transport Canada has adequate breach notification requirements for air carriers under the Treasury Board Guidelines for Privacy Breaches.

61. For personnel security we examined whether the security clearances held by Program employees were adequate for the nature and sensitivity of the information handled as required by the Treasury Board Personnel Security Standard.

62. For information technology security we examined the operational and development environments and access controls according to the Management of Information Technology Security standard.

63. We found that Transport Canada's overall approach to the protection of personal information stored within the Program ensured its security. Transport Canada operations for the Program is centralized. Program activities are conducted in secure areas, which are accessible by a small number of employees who possess adequate security clearances (secret or top-secret) and who have obtained training in information security. Security guards, access and ID cards, locks, containers and a clean desk policy are used to safeguard Program information within secure areas. Transport Canada has taken adequate steps to ensure perimeter and internal security of its information technology systems for the Program with one exception. We also observed two security problems with information disclosed to air carriers.

64. Our concerns with Transport Canada's existing safeguards within the Program relate to the Specified Persons List information technology application, the breach notification procedures with air carriers, and Transport Canada's oversight of air carriers' handling and safeguarding of Program information.

Transport Canada can not demonstrate that the Specified Persons List information technology application has been certified and accredited to meet the requirements of government security standards.

65. Air carriers must work with the most accurate list of names from Transport Canada at all times. The Specified Persons List application is the department's information technology system to distribute updates of Specified Persons List quickly to air carriers domestically and around the world, to ensure that passengers are being matched against current information.

66. We expected Transport Canada to follow the Management of Information Technology Security operational standard, which requires that government information technology systems undergo a Certification and Accreditation process.

67. Certification is to verify the security requirements established for an information technology system or service are satisfied and that the controls and safeguards work as intended. Accreditation is to ensure that management authorization has been obtained for the system or service to operate, including the acceptance of any remaining risk based on the certification process.

68. Transport Canada was unable to demonstrate that it has a formal Certification and Accreditation process for the Specified Persons List application as required by government information technology standards. This situation exposes the department to a risk that the system could house undetected security weaknesses which may affect the integrity of the personal information contained within the Program.

69. In testing how the application works, we found an example of one information technology control that was not functioning as intended. The control weakness related to a system programming change affecting access rights, which was implemented before the change was tested to confirm that it was working properly.

70. We observed that this lack of testing before implementation led to an undetected error that prevented authorized persons at Transport Canada from accessing data on the application. However, this control vulnerability may have resulted in the opposite occurring; that is to say, a person who would normally not have had the authority to update the List could have been mistakenly given such important access rights in error. If such a situation were to occur, it could lead to a privacy breach involving sensitive information.

71. The department informed us that it currently has information technology controls equivalent to a Certification and Accreditation process as part of its change management process. However, the programming error that occurred during the audit may have been prevented if a formal Certification and Accreditation process had been in place for the Specified Persons List application.

Recommendation: That Transport Canada complies with the government's information technology security requirements by creating a formal Certification and Accreditation process and subject the Specified Persons List information technology application to it.

Transport Canada's management response:

"Transport Canada is compliant with MITS. However, it has accepted to review its processes, and, as necessary, adjust them based on best practices/guidelines etc. for certification and accreditation. Transport Canada will subject the Specified Persons List information application to any revised certification and accreditation process by December 31, 2009."

There is no requirement for airlines to report data breaches.

72. A privacy breach may involve the improper or unauthorized collection, use, disclosure, modification and/or disposal of personal information. A single privacy breach by an air carrier involving sensitive Specified Persons List information could severely and negatively impact on the privacy of an individual or individuals named on the list. Such a breach could also seriously damage the public confidence in and reputation of the Passenger Protect Program. The Government Security Policy requires that government institutions take adequate measures to prevent privacy breaches involving Canadian's personal information.

73. Although there is no specific requirement for a third party, such as an airline, to report a privacy breach to the originator of that information such as Transport Canada, Treasury Board Secretariat's Guidelines for Privacy Breaches indicates that in the case of contracts, information sharing agreements with third-parties should include a "requirement to immediately notify the government institution of a privacy breach."

74. We expected that air carriers, as a best practice, would be required to report privacy breaches involving the handling of sensitive Specified Persons List information to Transport Canada.

75. We found that the Identity Screening Regulations with airlines does not require the reporting of privacy breaches to Transport Canada.

Recommendation: Transport Canada should amend its Identity Screening Regulations to require air carriers to report privacy breaches involving the handling or safeguarding of Specified Persons List related personal information to the Department.

Transport Canada's management response:

"Although there is currently no regulated requirement for air carriers to self-report any infractions committed, the department is moving to a Security Management System (SeMS) approach to aviation security. Under such an approach, air carriers would identify gaps and vulnerabilities within their operations, which could included safeguard and handling of the Specified Persons List related information. Air carriers would have to address any gaps, take appropriate measures to deal with them and monitor whether the measures to deal with them and monitor whether the measures implemented are effective.

Transport Canada is also conducting a review of all aviation security regulations, measures and standards. The requirement for self-reporting provisions may be considered in the context of this review."

Transport Canada has not verified that airlines are adequately protecting personal information.

76. As previously mentioned, our audit did not review air carriers personal information handling practices, but we did examine Transport Canada's role in overseeing air carriers' practices related to the access, collection, use, disclosure, accuracy and safeguarding of such information.

77. The Identity Screening Regulations contain a number of obligations related to air carriers' access, use, disclosure and accuracy of the Passenger Protect Program information.

78. We expected that Transport Canada's oversight activities would ensure that air carriers are properly handling and protecting personal information as required by the Identity Screening Regulations.

79. We noted that soon after the Passenger Protect Program began in 2007, Transport Canada's Aviation Security Operations began inspecting airlines at numerous airports around the world. In reviewing a sample of Transport Canada's inspection reports, we found that the department's oversight activities had focused primarily on the extent to which the airlines were using the Specified Persons List as a tool for screening passengers. We also found that the inspections did not focus on how the air carriers were handling and safeguarding the List in accordance with the Identity Screening Regulations.

80. We also found that two smaller airlines did not have an automated means to match passenger information with the Specified Persons List. These airlines print copies of the List for front line staff at the airports where they operate.

81. As Transport Canada has not carried out inspection activities over these airlines' handling and safeguarding of personal information, it cannot provide assurance that this sensitive personal information could not be used or disclosed inappropriately.

82. If the Specified Persons List were disclosed publicly, for instance, such a breach could have a serious impact on the persons named and on the reputation of the Passenger Protect Program.

Recommendation: Transport Canada should extend its regulatory oversight activities to verifying that airlines are complying with all requirements of the Identity Screening Regulations as they relate to the handling and safeguarding of Specified Persons List information.

Transport Canada's management response:

"Transport Canada agrees with the recommendation. Although not conducted at the time of the audit, as of June 2009 the department has been inspecting air carriers to verify compliance with all requirements of the Identity Screening Regulations as they relate to the handling and safeguarding of the Specified Persons List Information."

Conclusion

83. We conclude that in most material respects Transport Canada complies with relevant provisions of the *Privacy Act*, the *Aeronautics Act* and other regulations and policies for the handling and safeguarding of personal information within the Passenger Protect Program.

84. We did note, however, some important privacy vulnerabilities that warrant Transport Canada's management's attention:

- The Deputy Minister at Transport Canada was not provided with complete information when deciding to add or remove names to or from the Specified Persons List.
- The application used to transfer Specified Persons List information to air carriers has not undergone a formal certification and accreditation process.

- Air carriers are not required to report security breaches involving Passenger Protect Program related personal information to Transport Canada; and
- Transport Canada has not yet extended its oversight activities to verify that airlines are adequately handling and safeguarding Specified Persons List information disclosed by the department.

85. If these gaps are properly addressed, Transport Canada would strengthen its privacy and security management framework for the protection of Canadian's sensitive personal information within the Passenger Protect Program.

86. Transport Canada has responded positively to our recommendations relating to the Passenger Protect Program. The department has made changes to comply with recommendations dealing with information provided to the Deputy Minister and with the department's oversight role of airlines under the Program.

87. The department has also committed to undertake activities to improve its practices for the enhancement and protection of Canadians' sensitive personal information.

88. Finally, the department has committed to review its existing Certification and Accreditation processes and will adjust them based on best practices and guidelines. We continue to note, however, that Transport Canada did not demonstrate during the audit that it has a documented Certification and Accreditation process, as defined by the government security policies.

89. We will conduct a follow-up to this audit exercise in two years to verify the progress made by Transport Canada in implementing its plan in response to our recommendations.

About the Audit

Objective

The objective of the audit was to determine whether Transport Canada has adequate controls and safeguards in place for the personal information within the Passenger Protect Program.

Scope and approach

Audit activities were conducted at Transport Canada's headquarters in Ottawa. During our audit we examined the Program activities and documentation for the period from June of 2007 to March of 2009.

The audit scope extended to five program areas at Transport Canada, the: Specified Persons List Advisory Group, Intelligence Operations and Support Section, Information Technology Branch (including the Specified Persons List application), Office of Reconsideration and Aviation Security Operations.

The audit assessed Transport Canada's personal information handling and safeguarding practices and controls, throughout the life cycle of the information—from collection to disposal.

The audit did not extend to the verification of air carriers' handling and protection of personal information, but did examine Transport Canada's oversight role in verifying that the airlines were adequately handling and protecting personal information relating to the Passenger Protect Program.

As well, the audit did not evaluate the effectiveness of the Passenger Protect Program, nor did we assess the pertinence of adding specific individuals to the Specified Persons List or not, as these questions were outside the mandate of the Privacy Commissioner.

The audit approach with Transport Canada included the review of policies, practices, administrative controls and safeguards for the various program areas examined. Documents reviewed included various standard operating procedures, agreements, work-flow documents, training materials, forms and records retention documents.

We interviewed key management and front-line staff to gain a broad understanding of the Passenger Protect Program and its activities and to test their understanding of privacy and security.

We also visited various Transport Canada sites, examined Passenger Protect processes, reviewed program documentation such as inspection reports, incident reports, reconsideration files, and tested the Specified Persons List information technology application controls against our lines of inquiry.

Lines of Inquiry

1. We expected that Transport Canada would comply with sections 4, 5, 7 and 8 of the *Privacy Act* and would have controls for the collection, use and disclosure of personal information.
2. We expected that Transport Canada would comply with subsections 6(1) and (3) of the *Privacy Act* and would have controls for the retention and disposal of personal information.
3. We expected that Transport Canada would comply with subsection 6(2) of the *Privacy Act* and would have controls to ensure that personal information, used to make administrative decisions within the Passenger Protect Program is as accurate, up-to-date and complete as possible.
4. We expected that Transport Canada would comply with the government security policies, standards and related requirements, and use physical, personnel and information technology safeguards to protect personal information used in the Passenger Protect Program throughout its lifecycle.
5. We expected Transport Canada to oversee Passenger Protect Program activities as carried out by airlines, to ensure that Specified Persons List information is handled and protected in accordance with the Identity Screening Regulations and section 2 of the *Privacy Act*.

Standards

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

Audit Team

Director General Audit and Review: Steven Morgan
Audit Manager/Audit Lead: Tom J. Fitzpatrick
Senior Audit & Review Officer: Garth Cookshaw
Senior Advisor: William (Bill) Wilson