Enhanced Student Information System (ESIS): Addressing Privacy Concerns

Centre for Education Statistics
Statistics Canada

March 2001

INTRODUCTION

The Enhanced Student Information System (ESIS) is currently under development at Statistics Canada with the full support of the Canadian Education Statistics Council. One of the important objectives of ESIS is to follow student pathways through the education system. To achieve this objective, ESIS requires student identification information from the post-secondary institutions. Even though the results are confidential and protected by the *Statistics Act*, privacy concerns may arise because of underlying public concerns and perceptions about large databases holding information about individuals.

This document outlines the principles and procedures that Statistics Canada is putting in place for this project with respect to privacy. The Centre for Education Statistics has examined the ESIS project in the light of the code of fair information practices set out in the *Privacy Act* and, more recently, in the privacy principles established by Parliament in the *Personal Information Protection and Electronic Documents Act*. The principles are stated below, followed by the approach taken in ESIS to meet each one.

The principles were taken from Schedule 1 (Section 5) of *Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-830-96.*

The ten principles are: accountability, identifying purposes, consent, limiting collection, limiting use, disclosure and retention, accuracy, safeguards, openness, individual access and challenging compliance.

Each principle is reproduced below, followed by a statement in italics which explains Statistics Canada's approach.

PRINCIPLE 1: ACCOUNTABILITY

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

1.1 Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

In Statistics Canada this responsibility rests with the Director, Data Access and Control, who is the Coordinator, Access to Information and Privacy.

1.2 The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.

Information describing privacy issues as they relate to ESIS will be available on the Statistics Canada web site. That site will identify and provide coordinates for the Privacy Coordinator, who is the Director, Data Access and Control Services, as well as identify a specific contact person to obtain more information on ESIS. Some post-secondary institutions' registration forms already include notification that information will be provided to Statistics Canada. Steps can be taken to ensure that this practice becomes universal. Such statements can refer students to a more detailed statement in the calendar. In turn, the calendar can include a Statistics Canada website address for in-depth information.

1.3 An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

In many cases, post-secondary data are provided to Statistics Canada directly by institutions. Statistics Canada's preference is to work through coordinating bodies in each province, which also advances provinces' own needs for planning information. Work with coordinating bodies is already well advanced in Alberta, Quebec, and the member-provinces of MPHEC. Ontario and BC also have coordinating bodies that provide a point of contact for Statistics Canada. Alberta, Quebec, the Maritimes, and BC have worked with their institutions to define data needs, including requirements under the Statistics Act. Statistics Canada has been part of those meetings as appropriate. In Ontario, the situation has changed in recent years and Statistics Canada now works equally with the institutions and the Ministry of Training, Colleges and Universities. These arrangements might be understood as the province 'intercepting' data en-route to Statistics Canada. As provinces develop their own central databases to meet their own needs for comprehensive planning data, they will be able to meet Statistics Canada's needs directly. Such arrangements reduce institutions' reporting burden and reduce the risk of inconsistencies in the numbers 'on the street'.

Where ESIS data requirements exceed the data requirements of provinces and territories, memoranda of understanding can be negotiated between Statistics Canada and the ministries in question for the ESIS data required under Section 10 of the Statistics Act. Where provinces are involved in data transmission, Statistics Canada will make available to provinces, and to their institutions, software that meets or exceeds industry standards for the secure transmission of data.

1.4 Organizations shall implement policies and practices to give effect to the principles, including:

(a) implementing procedures to protect personal information;

Statistics Canada is prohibited under the Statistics Act from disclosing any information that would identify individuals. Measures to prevent unauthorized disclosure include: a computer environment where secure information resides on a physically separate network that does not communicate with the outside world; secure premises where non-Statistics Canada employees have to be signed in by an employee; storage of sensitive data such as ESIS on servers that are kept under lock and key and accessible only to a limited number of persons on a need-to-know basis. Most importantly, over generations, Statistics Canada has developed a culture where confidentiality of data is paramount, and that culture is continually reinforced.

(b) establishing procedures to receive and respond to complaints and inquiries;

As described in 1.2 above, there will be a number to call for complaints and inquiries.

(c) training staff and communicating to staff information about the organization's policies and practices; and

All Statistics Canada staff swear or affirm an oath of secrecy under the Statistics Act, and receive information on procedures and policies with respect to the protection of information. The Act and other relevant legislation and departmental policies are on the department's intranet site, where they are accessible to all employees.

(d) developing information to explain the organization's policies and procedures.

An interpretative document explaining the provisions of the Statistics Act is on the department's intranet site, accessible to all employees.

PRINCIPLE 2: IDENTIFYING PURPOSES

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

2.1 The organization shall document the purposes for which personal information is collected in order to comply with Principle 8 (Openness) and Principle 9 (Individual Access.)

Documentation on ESIS will be available on the Statistics Canada web site describing the purposes and objectives of ESIS and uses of the data. This documentation will also describe proposed linkages of ESIS and other data sets; the purpose of the linkage; and the controls in place at Statistics Canada on approval of record linkages and on the use and retention of linked files.

The possibility exists that ESIS may be linked to taxation files to study mid- to long-term returns to education, and to Canada Student Loans files to study issues of access and persistence. All record linkage proposals must satisfy a stringent review and approval process, which involves the submission of document proposals to a senior review committee.

The recommendations of the review committee are forwarded to the Chief Statistician, who refers for ministerial approval all recommendations he supports and which represent types of linkages not previously approved by the Minister. It is the Minister who (as a proxy for the general public) applies the ultimate judgement regarding the trade-off between the expected public benefit and the degree of privacy invasion which may be involved. Information resulting from record linkages, like all other statistical information, is protected by the confidentiality provisions of the Statistics Act.

A summary of the approved record linkages involving personal information is published in Statistics Canada's Annual Report on Access to Information and Privacy and will be available on the Statistics Canada web site.

2.2 Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfil these purposes. Principle 4 (Limiting Collection) requires an organization to collect only that information necessary for the purposes that have been identified.

ESIS was developed in consultation with stakeholders across Canada. These include the provinces, educational institutions, national organizations, and departments of the Government of Canada. All variables in the proposed ESIS database have an identifiable need, as described in 2.1. If any of those variables no longer meet an identifiable need they will be dropped.

2.3 The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

Notification of purpose by the original collectors of the information, i.e. the institutions themselves, will take the form of a note on student registration forms (as described in

1.2). Calendars will contain further information, including a reference to the Statistics Canada website where full documentation is available.

2.4 When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to Principle 3 (Consent).

Under the Statistics Act, ESIS will be used only for statistical, research, and analytical purposes, and will never be used for administrative purposes directly affecting a particular individual or in any fashion that identifies individuals. Statistics Canada is a protected data enclave, and no other government department or organization has the authority to require Statistics Canada to provide access to any identifiable personal information collected by the Agency, including ESIS. A number of statistical, research, and analytical uses of ESIS have been identified at this time. If other such uses are identified in the future, they will be described on the Statistics Canada website. If new uses involve linkage to other information, the new use will be subject to the record linkage approval process at Statistics Canada.

2.5 Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

2.6 This principle is linked closely to Principle 4 (Limiting Collection) and Principle 5 (Limiting Use, Disclosure and Retention).

The Statistics Canada website will provide the name and contact information for an individual who will be able to fully explain the data needs met by ESIS. Contacts in institutions and in education ministries involved in the collection and reporting of ESIS information will be fully advised on the purposes of ESIS, so that they, too, are able to answer questions.

PRINCIPLE 3: CONSENT

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate. Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor,

seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.

3.1 Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

3.2 The principle requires “knowledge and consent”. Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

3.3 An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.

3.4 The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

3.5 In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care

professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

3.6 The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

3.7 Individuals can give consent in many ways. For example:
(*a*) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;
(*b*) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;
(*c*) consent may be given orally when information is collected over the telephone; or
(*d*) consent may be given at the time that individuals use a product or service.

3.8 An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

Because the original collection of the information occurs at the time the student registers with the institution, the process for informed consent will work as follows. Details of this implementation have yet to be worked out with individual institutions.

(a) Notification of use of registration information for statistical purposes will appear on the registration form completed by students. Where possible, this notice will reference the calendar as a source of further information on the uses of the information for statistical purposes.

(b) The calendar will contain a brief description of the importance of the information for planning and policy development, and the role of Statistics Canada. The purpose of ESIS and the use of student data in ESIS will be noted; the description will include examples of statistical, research, and analytic uses of the information. Safeguards to prevent the disclosure of personal information will also be briefly described. In turn, that note in the calendar can include a Statistics Canada website address, where additional information can be obtained.

(c) The Statistics Canada website will contain detailed information on ESIS, its purpose and uses, approved linkages to other data sets, and procedures and controls to prevent disclosure of information at Statistics Canada.

(d) The web site will provide the name and contact information for an individual who will be able to fully explain the purposes for which the ESIS information is being collected.

(e) The Statistics Canada contact person will be authorized to invoke an "opted-out status" for any individual who objects to the inclusion of his or her personal information in ESIS, and to erase personal identifier information for those who invoke an opted-out status. The need for retaining the individual's record exclusive of personal identifiers relates to the principle of accuracy. ESIS needs to provide accurate statistical measures of post-secondary education, including enrolment and graduation counts and participation rates, and this cannot be achieved unless information on all students is included.

PRINCIPLE 4: LIMITING COLLECTION

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

4.1 Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with Principle 8 (Openness).

4.2 The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

4.3 This principle is linked closely to Principle 2 (Identifying Purposes) and Principle 3 (Consent.).

Access to data collected by institutions for ESIS reporting purposes will be limited to information necessary for the purposes identified.

Access to data collected by institutions for ESIS reporting purposes is fair and lawful in accordance with the provisions of the Statistics Act.

The use of Social Insurance Numbers (SIN) is proposed. The need for SIN relates to the accuracy principle. Without SIN the ability to accurately link records of individual students over time when they change the province and/or institution of study would be limited. This would compromise one of the purposes of ESIS, namely to better monitor and understand student flows and pathways within post-secondary education. Without SIN, the linkages possible using name and date of birth information would not be sufficiently accurate to undertake certain types of studies, for example, the possible linkage of historical student records with current tax files to examine the distribution of incomes by field of study 10-20 years after graduation. The combinations of errors or lack of standardization in the name, errors in date of birth, and the instances of name changes over time (particularly of women) would render unacceptable the accuracy of such a linkage.

*Federal legislation and policy, while restricting the use of SIN for **administrative** purposes, does not prohibit its use for statistical purposes. While there is a clear and demonstrable benefit to the use of SIN in ESIS in meeting its purpose and objectives, individuals can invoke an "opted-out status" and all personal identifier information, including the SIN, will be erased from ESIS (see 3.8). It is worth noting that SIN is already collected in many current systems for collection of student level data, except in Quebec. The SIN has been used to verify information with the bodies reporting data, for studies of mobility, and for estimating a 'national graduation rate'; with respect to the latter, the SIN has been used for the latter purpose since 1974.*

PRINCIPLE 5: LIMITING USE, DISCLOSURE AND RETENTION

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

5.1 Organizations using personal information for a new purpose shall document this purpose (see 2.1).

5.2 Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access

to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

Individuals will be maintained on the live ESIS database for twenty years following their most recent year of enrolment in a post-secondary institution. Individuals who have not been active in pursuing their education after the lapse of twenty years will have their records transferred to an archival database. Should such an individual resume enrolment after a break, the individual's records would be re-instated to the live database.

The need for archival records stems from the need for the study of student flows over a very long term and for study of long-term returns to education. The former would be done by linking the ESIS database over years. It is proposed to do the latter by linking a sample of ESIS to the tax file, which is held at STC under controlled conditions for statistical purposes. These studies would examine taxable income of individuals by field of study at various intervals after completion of studies. These studies would be subject to approval on a case-by-case basis by the Chief Statistician, in compliance with Statistics Canada's record linkage policy. (See 2.1.)

5.3 Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

5.4 This principle is closely linked to Principle 3 (Consent), Principle 2 (Identifying Purposes) and Principle 9 (Individual Access).

Statistics Canada will examine the feasibility of establishing a destruction date for records of individuals. This is complicated by the increasing policy interest by governments and professional associations in the notion of lifelong learning, and the need to be able to track learning of individuals throughout life, even after long breaks (e.g., an individual who pursues further studies after their retirement from the labour force).

PRINCIPLE 6: ACCURACY

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

6.1 The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the

individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

Under the Statistics Act, ESIS will be used solely for statistical purposes. No use will be made of ESIS data to make decisions about a specific individual.

Nevertheless, accuracy of ESIS information is important if statistical findings are to be valid. For this reason, the ESIS processing system has validity checks and edits built into it. Institutions providing ESIS data have access to a "pre-screener", which identifies most data irregularities, so they can be fixed before the data are sent.

Under the Privacy Act, individuals have the right to request correction of their personal information where they believe there is an error or omission. This applies only where the personal information has been used, is being used or is available for use for an administrative purpose (reference subsection 12(2) of the Privacy Act). Since information collected for purposes of the Statistics Act is not used for administrative purposes, it is very rare that someone would request a correction be made to their record.

6.2 An organization shall not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.

Statistics Canada will only update personal information on the ESIS database using updates provided through continued ESIS reporting.

6.3 Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

Personal information on ESIS will be kept up-to-date through ongoing ESIS reporting, and will not be disclosed to third parties.

PRINCIPLE 7: SAFEGUARDS

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

7.1 The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

Statistics Canada has a comprehensive set of policies and practices in place to ensure the protection of all information collected or obtained for the purposes of the Statistics Act. See examples in 1.4.

7.2 The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in 3.4.

All information protected by the confidentiality provisions of the Statistics Act, including ESIS, is subject to the security policies and practices of Statistics Canada.

7.3 The methods of protection should include:

(a) physical measures, for example, locked filing cabinets and restricted access to offices;

Physical measures include restricted access to offices. Employees are required to apply to Statistics Canada's security office for an identity card, to display these to commissionaires on entry to the premises, and to display their badges at all times while on the premises. Entry outside of regular working hours is restricted to employees with off-hours authorization, and such employees must sign in and out. Any printouts of ESIS records will be kept under lock and key when not in direct use by authorized employees.

(*b*) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and

All Statistics Canada employees are sworn in under the Statistics Act and subject to its criminal sanctions for unauthorized activities. The server where the ESIS database resides is kept in a locked room, and access to it is restricted to small number of staff working on ESIS.

(*c*) technological measures, for example, the use of passwords and encryption.

Institutions and jurisdictions use encryption when providing ESIS data to Statistics Canada. Institutions transfer their data electronically to Statistics Canada using encryption software that meets or exceeds the most recent industry standards for

the secure transmission of data. The ESIS database is password-protected at multiple levels. The ESIS database resides behind a firewall using the latest in firewall technology and is physically separated from the external network. Backups are handled and stored in a secure manner. All ESIS files will reside on a server and not on individual workstations. Individuals with access to the server are prohibited from having access via the external network; that is, they cannot work on the data from any site outside the Statistics Canada building, including their home.

7.4 Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

All employees are made aware of the importance of maintaining the confidentiality of personal information. This is achieved through the swearing in under the Statistics Act, information on the intranet site, and constant reinforcement of the corporate culture by the Chief Statistician, Assistant Chief Statisticians, and all senior staff.

7.5 Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see 5.3).

Statistics Canada has in place procedures for shredding sensitive paper information. Procedures are also in place for the secure disposal of backups and copies of databases – and portions of databases - such as ESIS, once they are no longer required.

PRINCIPLE 8: OPENNESS

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

8.1 Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

All information regarding the policies and practices with respect to management of personal information within ESIS will be described in plain language on the Statistics Canada web site.

8.2 The information made available shall include
(*a*) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;
(*b*) the means of gaining access to personal information held by the organization;
(*c*) a description of the type of personal information held by the organization, including a general account of its use;
(d) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and
(e) what personal information is made available to related organizations (e.g., subsidiaries).

As required by the Federal Access to Information and Privacy legislation, a description of the Agency's information holdings including personal information banks is published annually in the Treasury Board publication Info Source: Sources of Federal Government Information. This also sets out how individuals may request access to their personal information under the Privacy Act.

8.3 An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

PRINCIPLE 9: INDIVIDUAL ACCESS

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Note: In certain situations, an organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

9.1 Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are

encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

Statistics Canada complies with the above. See 8.2.

9.2 An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.

9.3 In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.

Statistics Canada only provides personal information to third parties when the respondent has explicitly agreed to such a disclosure under very strict provisions of the Statistics Act.

9.4 An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.

Statistics Canada is in compliance. As a federal government institution, Statistics Canada is subject to the Privacy Act. Requests from individuals for access to their personal information must be treated in accordance with that Act, and would normally result in their information being provided to them.

9.5 When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

Statistics Canada is in compliance. See 6.1.

9.6 When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.

Statistics Canada is in compliance. See 6.1.

PRINCIPLE 10: CHALLENGING COMPLIANCE

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

10.1 The individual accountable for an organization's compliance is discussed in 1.1.

10.2 Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.

10.3 Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory bodies accept complaints about the personal-information handling practices of the companies they regulate.

10.4 An organization shall investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.

Under the Privacy Act, individuals may complain to the Federal Privacy Commissioner if they do not believe the institution has responded appropriately to their concerns. Such complaints would be investigated by the Office of the Privacy Commissioner.