AUDIT OF FAMILY LAW ASSISTANCE SERVICES

Report presented to the Departmental Audit Committee
by Internal Audit Services
Department of Justice Canada

Approved by the Deputy Minister on March 28, 2017

ISBN 978-0-660-08593-7
Cat. No. J2-451/2017E-PDF

Table of Contents

Executive Summary

Introduction

At the Department of Justice Canada (the Department), matters of family law are led by the Family, Children and Youth (FCY) Section in the Policy Sector. FCY bears responsibility for the federal government's mandate under the *Divorce Act*, the *Family Orders and Agreements Enforcement Assistance Act* (FOAEAA), and the *Garnishment, Attachment and Pension Diversion Act* (GAPDA), among others.

While FCY is chiefly concerned with legal and policy matters, operational duties under these acts have been assigned to FCY's Family Law Assistance Services (FLAS) unit, which is responsible for the administration and operation of three primary programs:

1) The Central Registry of Divorce Proceedings (CRDP), a nation-wide registry of divorce proceedings established to detect duplicate proceedings;
2) The Family Orders and Agreements Enforcement Assistance (FOAEA) program, which assists in the tracing of individuals in default of family obligations, the interception of federal payments, and the suspension of federal licences such as Canadian passports and federal marine and aviation licences; and
3) The Garnishment, Attachment and Pension Diversion Registry for the National Capital Region (GAPDA program), which validates applications for the garnishment of federal public servants' salaries and provides instructions to departmental compensation offices.

In addition to the administration of the above three operational programs, FLAS is responsible for the FCYinfoline, an information service available to the general public in support of family law and family violence issues.

As an operational unit, FLAS stands out from the Department's core responsibilities for legislative reform, policy development, and litigation support. Not only does it provide an essential service in the enforcement of family orders, it bears central responsibility for important statutory obligations imposed on the Minister of Justice. FLAS is also the steward for the Department's only mission-critical system[1], the FOAEA system, which holds large volumes of sensitive personal information.

The objective of the audit was to provide assurance that:

a. Governance mechanisms are in place to support the administration of the CRDP, FOAEA and GAPDA programs;
b. Privacy controls are designed to help ensure the proper[2] handling of personal information; and
c. Controls are designed to support the integrity of information and data in the FOAEA system.

To achieve this objective, the audit assessed the design of privacy controls over all FLAS operations. Also, in recognition of FLAS' use of the FOAEA system, information technology (IT) general controls over the garnishment process supported by the system were also assessed. The audit covered FLAS activities for fiscal years 2014-15 and 2015-16.

[1] A mission-critical system is an information technology system that is essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government.
[2] 'Proper' in this context means the handling of personal information in compliance with sections 4 through 8 of the *Privacy Act*, and in a manner that is appropriate in the circumstances.

Strengths

Overall, we found FLAS to be a well-managed unit. It operates effectively and efficiently despite a lack of permanent funding, which, according to management, makes day-to-day management difficult at times. Employees have a clear sense of their duties and continuously meet or exceed established service standards. From a privacy perspective, they have a firm appreciation of the sensitivity of their information holdings, and treat personal information under their custody and control with care and consideration.

Areas for Improvement

While FLAS has made strides in improving operations, the audit identified areas for improvement. First, despite significant investments in technology, FLAS continues, in some cases, to use manual processes that are comparatively more costly and time-consuming than their electronic alternatives. The use of manual processes also increases the risk of an error or a mishandling of personal information.

The audit also identified areas for improvement in governance and internal controls. From a governance perspective, FLAS could benefit from improvements in performance measurement. From an internal controls perspective, FLAS could benefit from a review of select privacy risk mitigation practices, and the mitigation of IT concerns.

Opportunity

In operating the FOAEA, CRDP and GAPDA programs, FLAS generates data on Canadian families that is of interest to a number of stakeholders including academics, researchers and policy groups. This data could also be useful to provinces and territories and their respective maintenance enforcement programs, allowing them to make more informed decisions about matters that affect families across Canada. At this time, the Department is not sharing FLAS data with these stakeholders.

In light of the Government of Canada's Open Data initiative, there is now an opportunity for the Department to revisit its policy on sharing aggregate data for research, statistical and policy purposes. It could explore the possibility of anonymizing and de-identifying data in order to share FLAS information both inside and outside of government to increase transparency while still respecting the privacy of individuals.

Audit Opinion and Conclusion

In my opinion, the Department has effective governance mechanisms in place to support the administration of the CRDP, FOAEA and GAPDA programs. Privacy controls are designed to help ensure the proper[3] handling of personal information, and overall, the Department is meeting its obligations under the *Privacy Act* with respect to the handling of personal information by FLAS. Controls are designed to support the integrity of information and data in the FOAEA system. Opportunities for improvement to further mitigate risks exist and management has demonstrated a strong commitment and proactive approach to making improvements as issues arise.

[3] 'Proper' in this context means the handling of personal information in compliance with sections 4 through 8 of the *Privacy Act*, and in a manner that is appropriate in the circumstances.

Management Response

Management has responded to the recommendations per the management action plan, which is integrated into this report.

1. Statement of Conformance

In my professional judgment as Chief Audit Executive, the audit conforms to the *Internal Auditing Standards for the Government of Canada*, as supported by the results of the Quality Assurance and Improvement Program.

Submitted by:

Original signed by Inanc Yazar
March 28, 2017

Inanc Yazar, CPA CGA, CIA, CRMA
Chief Audit Executive
Department of Justice Canada

2. Acknowledgement

The Chief Audit Executive would like to thank the audit team and those individuals who contributed to this engagement. She would also like to thank the Director of FLAS for her cooperation and hard work in facilitating the conduct of the audit, over and above her ordinary work responsibilities.

As part of the audit, Internal Audit Services (IAS) collaborated with the Department's Financial Policy and Controls Division so as to leverage findings from a recent monitoring exercise of the Family Law Liability financial account. The collaboration was also intended to minimize the duplication of work and to reduce audit fatigue. Relevant findings from a recent IT security audit were also considered as part of IAS' environmental scan of FLAS' IT environment. We wish to also acknowledge contributions of officials from the Management and Chief Financial Officer Sector to our audit findings.

3. Background

Under Canada's Constitution (the *Constitution Act*, *1867*), federal, provincial, and territorial governments share jurisdiction over family law. As a result, Canadian families experiencing separation or divorce may be impacted by both federal and provincial/territorial legislation, along with each jurisdiction's respective policies and programs. A married couple applying for a divorce, for example, will be subject to the *Divorce Act*, a federal law which sets out the grounds for divorce and provisions for corollary relief [i.e., child support, spousal support, and parenting arrangements (custody and access)]. Depending on the specific issues in the case, that same couple may also be subject to provincial/territorial laws (such as the *Family Law Act* in Ontario), which cover a host of other family law matters, including the rights of spouses and dependents in regard to property.

Since family law is an area of shared jurisdiction, the Department of Justice Canada (the Department) works closely with provinces and territories in relation to family law matters to foster collaboration and partnerships, support improvements and innovation in family law services, and facilitate public legal education. Together with its provincial and territorial partners, the Department helps to mitigate the negative effects of separation and divorce on families and children.

Family law matters at the Department are led by the Family, Children and Youth (FCY) Section, situated within the Policy Sector. It bears responsibility for the federal government's mandate under the *Divorce Act*, the *Family Orders and Agreements Enforcement Assistance Act* (FOAEAA) and the *Garnishment, Attachment and Pension Diversion Act* (GAPDA), among others. While FCY is primarily concerned with legal and policy matters, operational responsibilities under these acts have been assigned to FCY's Family Law Assistance Services (FLAS) unit. FLAS employs 13 full-time equivalents (including temporary and casual help) and is responsible for the administration and operation of three primary programs:

- **The Central Registry of Divorce Proceedings (CRDP)**

  The CRDP is a nation-wide registry of divorce proceedings, established under the CRDP Regulations, designed to assist courts in Canada in determining jurisdiction by detecting duplicate divorce proceedings. Upon the filing of an application for divorce in a provincial/territorial court, the registrar of the court must submit an application for registration of divorce proceedings to the CRDP. If and when more than one application is filed for the same marriage, the CRDP, through its supporting system and processes, notifies the relevant provincial and territorial courts of the duplication as required under the CRDP Regulations, including the date that each divorce proceeding was filed so that the court can make a determination of jurisdiction. In 2015-16, FLAS processed 72,925 applications for registration of divorce proceedings received from the various courts and 73,331 disposition reports.

- **Family Orders and Agreements Enforcement Assistance (FOAEA)**

  The FOAEA program assists provincial/territorial maintenance enforcement programs (MEPs) and creditors in the enforcement of family support debts by virtue of the administration of the FOAEAA. The program processes applications received under FOAEAA to:

  1) Locate individuals who are in breach of a family provision (part I);
  2) Garnish federal monies should they become payable to individuals in default of their family support obligations (part II); and
  3) Suspend or deny issuance of federal licenses and Canadian passports in the name of individuals who are chronically in default of their family support obligations (part III).

  Garnishment applications make up the most significant part of FLAS' work; approximately 80% of applications submitted annually to FLAS are for the garnishment of federal monies. In 2015-16, $188,772,041 was garnisheed from federal monies that became payable to individuals named in those applications and distributed to Canadian families to satisfy family support debts.

- **Garnishment, Attachment and Pension Diversion Registry for the National Capital Region (GAPDA program)**

  FLAS' role in the GAPDA program is limited to the validation of applications for the garnishment of federal public servants' salaries and payments to federal contractors. FLAS is responsible for accepting and reviewing GAPDA applications, and providing instructions and advice to the departmental compensation offices responsible for processing the garnishment of public servant salaries. In 2015-16, FLAS processed 556 applications for garnishment and an additional 2,058 applications for terminations, amendments, and bankruptcies.

In addition to the administration of the above three operational programs, FLAS is responsible for the FCYinfoline, an information service available to the general public in support of family law and family violence issues.

In operating its CRDP, FOAEA and GAPDA programs, FLAS collaborates with parties that are both internal and external to the Department. Internally, FLAS collaborates with, and is supported by, other units within FCY. Given that a large part of the FOAEA program's workflow is automated (and/or dependent upon electronic exchange between partners), FLAS also works closely with an information technology (IT) team within the Information Solutions Branch (ISB).

Externally, FLAS works closely with provinces and territories. Its key partners or clients include provincial and territorial MEPs and family courts. MEPs are responsible for the enforcement of support orders and agreements and FLAS provides services to help MEPs enforce family obligations. FLAS also works closely with federal departments and agencies, particularly in the administration of the FOAEAA and Part I of the GAPDA. Federal partners include the Canada Revenue Agency (CRA), Employment and Social Development Canada (ESDC), Transport Canada (TC), Immigration, Refugee and Citizenship Canada (IRCC), and Public Services and Procurement Canada (PSPC).

In 2015-16, expenditures for the FLAS unit totaled $1,629,578. While this represents less than 1% of the Department's annual budget ($702 million in 2015-16), the unit's programs support Canadian families and family laws. FLAS provides a number of essential services in the family law sector and bears central responsibility for statutory obligations imposed on the Minister of Justice under the *Divorce Act*, the FOAEAA, the CRDP Regulations and the GAPDA. FLAS is also central to the coordination and integration of federal and provincial responsibilities for divorce proceedings and support enforcement.

In light of the importance of services provided by FLAS to provinces and territories – and by extension to Canadian families – the Department must ensure that FLAS is meeting its statutory obligations. Moreover, since the unit handles a high volume of very sensitive data, it is important for the Department to be vigilant in preserving data integrity and the protection of personal information under FLAS' custody and control. To support the aforementioned operational expectations, the audit examined governance mechanisms as well as privacy and information technology general controls as communicated in the following audit objective.

4. Audit Objective

The objective of this audit was to provide assurance that:

a. Governance mechanisms are in place to support the administration of the CRDP, FOAEA and GAPDA programs;
b. Privacy controls are designed to help ensure the proper[4] handling of personal information; and
c. Controls are designed to support the integrity of information and data in the FOAEA system.

5. Audit Scope

The focus of the audit was on fiscal years 2014-15 and 2015-16.

[4] 'Proper' in this context means the handling of personal information in compliance with sections 4 through 8 of the *Privacy Act*, and in a manner that is appropriate in the circumstances.

The scope of the audit included an assessment of privacy controls in place for all three FLAS programs so as to help ensure that the Department is in compliance with the *Privacy Act* and its supporting policies and directives.

The scope also included other internal controls, such as the monitoring of data entry. In addition, IT general controls focused on the garnishment process under Part II of the FOAEAA, which is the most significant operation of the FLAS unit.

An environmental scan conducted by IAS of FLAS' IT environment highlighted the need to segregate duties and ensure that FOAEA system data is being transmitted internally in a manner that is commensurate with the security level of the data. These actions, which are both widely recognized in IT management as being fundamental controls that reduce the risk of wrongdoing, were examined in this audit.

In light of the dependencies between FLAS and other units within FCY (e.g., Support Enforcement Law and Policy Unit, Family Law and Policy Unit), the scope included other units within FCY that directly support FLAS operations, where applicable. While the audit included agreements with partners, and data transmission controls, the scope was limited to the activities under the mandate of the Department.

6. Audit Approach

The audit team carried out its mandate in accordance with Treasury Board's *Policy on Internal Audit* and the *Internal Auditing Standards for the Government of Canada*. The audit employed various techniques including a risk assessment of the audit entity, interviews, system walkthroughs, and the review and analysis of documentation.

7. Findings, Recommendations and Management Action Plan

This section outlines observations and recommendations resulting from the audit work performed. For ease of review, observations and recommendations have been structured along the lines of enquiry and audit criteria identified in the planning phase of the audit. For a list of audit criteria please refer to Appendix A.

7.1 Governance Mechanisms

The audit examined the extent to which governance mechanisms are in place to support the administration of FLAS' CRDP, FOAEA and GAPDA programs. By 'governance mechanism,' we mean the processes, procedures and structures implemented to help manage and oversee the unit's core operating activities. Our review included an examination of FLAS' strategic planning efforts, the study of program measurement activities, inquiries into roles and responsibilities, and a review of governing agreements with federal, and provincial and territorial, partners. Good governance leads to better decision making. It also helps to ensure that the Department is fulfilling its legislative responsibilities.

Finding 1:

FLAS has sufficient strategic planning activities in place and communicates operational roles and responsibilities to support the administration of its operating programs. However, opportunities exist to improve FLAS' performance measurement activities, and to update governing agreements with key program partners.

Linkage to: Governance

Performance Measurement

Performance measurement is the systematic collection and analysis of program outcomes, used to make decisions about a program's overall performance. The collection and analysis of program outcomes, where properly identified, enables managers to make more objective and timely decisions regarding a program's performance and direction.

FLAS demonstrates results-oriented practices and culture by consistently tracking and reporting on performance. As part of the audit, we reviewed and analysed the performance indicators being used by management to evaluate the activities of the CRDP, FOAEA and GAPDA programs. In order to report on and communicate key accomplishments to its federal, and provincial and territorial stakeholders, each year FLAS prepares a comprehensive report of its core operating activities. In the report, the unit tracks a series of measures designed to demonstrate the success of each of its core programs. These measures are also outlined in the draft Performance Measurement and Evaluation Strategy, jointly developed by the FCY Section and the Department's Evaluation Division for the FCY as a whole.

While the performance measures reported by FLAS help quantify the kind of work performed by FLAS, they are volumetric in nature and fall short of measuring the unit's performance. Put more simply, while FLAS is actively measuring 'how much' work they do, they are not measuring 'how well' that work is being done. For example, FLAS currently measures the total number of calls received for CRDP proceedings, the total number of applications for garnishment processed under the FOAEAA, the total dollar figure of funds garnished from federal funds, the number of applications for the denial and suspension of passports and federal licences, and the number of calls received by the FCYinfoline. The unit does not however report the average number of days in which applications were processed, the rate of errors identified in CRDP proceedings, or the turnaround period for tracing applications. In our view, these are important measures of program success.

In order to ensure that the unit is meeting its statutory obligations, and is working to advance the broader obligations of the Department, FLAS would benefit from a re-evaluation of the performance metrics it uses to measure program success in its annual report. In doing so, FLAS and FCY should continue to work closely with the Department's evaluation and performance measurement functions so as to ensure that performance metrics are established against key service standards, as defined in governing acts, regulations, and federal and provincial/territorial agreements. While FLAS stated meeting all such standards, the unit's success in doing so is not being actively reported. Performance measures should also take into consideration the needs of internal and external stakeholders. For instance, internal stakeholders need to track program success and external stakeholders' needs may include measuring FLAS' impact on child poverty, Canadian families, etc. By establishing and measuring a more comprehensive set of performance measures, FLAS will be better positioned to demonstrate program success.

Governing Agreements

A written information sharing agreement is intended to serve as a written record of understanding between parties that outlines the terms and conditions under which personal information is to be collected, used, disclosed, safeguarded and retained.

In determining whether FLAS has such agreements in place with key program partners, IAS reviewed a listing of all signed memoranda of agreement with provinces and territories for the administration of both the CRDP and FOAEA programs. IAS also reviewed copies of governing terms of reference for the use of FOAEA services by provincial partners, and memoranda of understanding with key federal partners for FOAEA program operations.

On the whole, the audit found that agreements governing the exchange of personal information are out of date. Most agreements between the Department and its provincial/territorial partners governing the exchange of data under Part I of FOAEAA were signed in the 1980s. These agreements, which in many cases predate the advent of the Internet and electronic communication, lack provisions prescribing roles, responsibilities and requirements for the proper handling of personal information. While some agreements include general provisions mandating data confidentiality, those provisions fall well short of modern-day expectations for the safeguarding of personal information [as set out in Treasury Board Secretariat (TBS) guidelines].

In addition to agreements with provincial partners, FLAS has formal memoranda of understanding in place with its key federal partners for FOAEA program operations: Passport Canada (now under IRCC), TC, CRA, and ESDC. As mentioned by management, FLAS has been working extensively with CRA and ESDC since 2009 to renew existing agreements (one of which dates to 1987). Despite all efforts to finalize the new arrangements, draft agreements remain unsigned.

Given the current state of the Department's agreements with its partners, roles and responsibilities for the exchange and handling of personal information remain unclear. As a result, FLAS or its partners may be susceptible to a mishandling of personal information. Outdated agreements for data handling may also create difficulties in the enforcement and monitoring of good privacy practices.

Recommendation 1	Management Action Plan
It is recommended that the Senior Assistant Deputy Minister, Policy Sector: a. Update performance measures used to measure the unit's success to include key service standards, as set out in governing acts, regulations and federal and provincial/territorial agreements, and to better reflect the reporting needs of key internal and external stakeholders; and b. Using a phased-in approach based on risk, update existing agreements with program partners to include privacy and security provisions.	Management agrees with the recommendation. a. Service standards reported in the Departmental Performance Report were revised in 2015-16 to better align with the collection of user fees under the CRDP and the FOAEA programs. A review of FLAS' current performance measures will be conducted to help determine which indicators would serve best to measure its progress and efficiencies and meet any reporting requirements linked to the Evaluation of the FCY Section and expectations of FLAS' clients. b. The procedures for the exchange of personal information, security measures and privacy risks management are detailed in formal agreements with each partner involved in the delivery of its services. The CRDP Regulations dictate the information that must be exchanged between

the courts and the CRDP to allow for the detection of duplicate divorce proceedings. Updated agreements setting out the current secure processes for the exchange of information between the provincial/territorial courts and the CRDP have been negotiated. To date, nine jurisdictions have signed the updated agreement. It would be worthwhile to note that unsigned, updated agreements in the remaining jurisdictions do not impede the registration and detection process described in the CRDP Regulations. However, management agrees that signed, updated agreements would explicitly clarify and communicate accountabilities related to the exchange of personal information with all of its provincial/territorial partners.

The FOAEA program cannot be delivered in isolation by the Department of Justice. The Act imposes legal obligations on other federal Ministers. Management has been working actively with federal partners involved in the delivery of the FOAEA program to negotiate updated information sharing agreements reflecting current practices, including the secure federally approved electronic processes in place to safeguard the information exchanged. Agreements with the Passport program and TC have been renewed; negotiations are ongoing with CRA and ESDC. While the lack of renewed agreements with all of its federal partners does not prevent FLAS from delivering its mandated enforcement services within secure environments, the signing of new agreements would ensure that accountabilities related to the exchange and security of personal information align with Treasury Board's recommended practices.

Under part I of the FOAEAA, locate information cannot be shared with an applicant unless the Minister of Justice is satisfied that the safeguards established by the agreement with the province are in place. Agreements with each province and territory were signed in the 1980s. These agreements are still in place and authorize the locate information under the FOAEAA to be provided to each applicant. Supplemental agreements dealing specifically with the exchange and handling of personal information with provincial/territorial partners under the FOAEAA will be negotiated to reflect modern-day expectations and [redacted] in place for the handling and safeguarding of personal information. In the event of amendments to the FOAEAA, the agreements themselves would be updated. This would provide assurances that information is released only for stated purposes while ensuring that the privacy intrusion is as

	limited as possible. No federal/provincial/territorial agreement is required under the garnishment (part II) and licence suspension (part III) provisions under the FOAEAA.
Office of Primary Interest:	Senior Assistant Deputy Minister, Policy Sector
Due Date:	• Completion of a review of performance measures for FLAS' programs by March 31, 2018. • Implementation of revised performance measures, as required, by March 31, 2019. • Updated agreements: o Updated agreement with CRA: December 2017. o Updated agreements with ESDC: March 31, 2019. o Agreements under Part I, FOAEAA: Supplemental agreements dealing specifically with the exchange and handling of personal information with provincial/territorial partners under the FOAEAA will be negotiated by March 31, 2018. In the event of amendments to the FOAEAA, the agreements themselves will be updated within three (3) years of the applicable provisions coming into effect.

7.2 Controls over the Handling of Personal Information

The audit examined the extent to which FLAS has designed controls to help ensure the proper handling of personal information, in keeping with the Department's obligations under sections 4 through 8 of the *Privacy Act*. We also examined the extent to which the unit had implemented TBS policies supporting the Act's administration. The audit included a review of privacy notices, and controls used to limit the collection, use, disclosure and retention of personal information. It also included an assessment of the design of controls used to help ensure the accuracy and completeness of personal information. We also surveyed controls in place to safeguard FLAS data from unauthorized use or disclosure. The proper handling of personal information helps to ensure the privacy of individuals whose information the unit uses for administrative purposes.

Finding 2:

FLAS is generally meeting its obligations under the *Privacy Act* and its supporting policies and directives. Opportunities for improvement were identified to strengthen the handling of sensitive information.

Linkage to: Controls

The audit found that FLAS is generally meeting its obligations under the *Privacy Act* in terms of the collection, use and disclosure of personal information. The unit is limiting its collection of personal information to that which is authorized by law, and personal information is not being used or disclosed for unrelated or secondary purposes. FLAS processes personal information according to formally documented policies and procedures, and system controls are used to protect and ensure the integrity of data. Opportunities exist to improve privacy notices, perform privacy impact assessments, and reduce reliance on manual processing.

Privacy Notices

Subsection 5(2) of the *Privacy Act* requires the Department to inform individuals from whom it intends to collect personal information of the purposes for which that information is to be collected. Section 6.2.9 of the TBS *Directive on Privacy Practices* requires privacy notices to state "the purpose and authority for the collection [of personal information]; any uses or disclosures that are consistent with the original purpose; any legal or administrative consequences for refusing to provide the personal information; the rights of access to, correction and protection of personal information under the [*Privacy*] *Act*; and the right to file a complaint to the Privacy Commissioner of Canada regarding the institution's handling of the individual's personal information." As a best practice, notification should be provided prior to, or at the time of, collection.

When personal information is collected directly from the individual, privacy notices are generally posted on the forms used for the collection of that information (whether paper or electronic). Where information is collected indirectly, the Department may rely on third party notices but must also disclose the purposes of collection in its personal information bank (PIB) descriptions. PIBs are indexes of the Department's personal information holdings, published annually and online in Info Source (a series of publications and databases containing information about the Government of Canada).

As part of the audit, IAS obtained copies of all forms used by FLAS for the collection of personal information. We also obtained copies of relevant system notifications for CRDP and FOAEA. Based on a review of those notices, and a comparison of those notices with the reporting requirements set out in the TBS *Directive on Privacy Practices*, the unit is meeting most, but not all, of its obligations for notification. Existing privacy notices do not always contain the minimum requirements set out by TBS, and some privacy notices were absent altogether.

As per management, the vast majority of information collected by the unit is collected indirectly from its program partners (i.e., MEPs under the FOAEAA, and provincial courts for CRDP). As such, privacy notices on select forms were deemed unnecessary. According to FLAS, the Department fulfills its obligations for informing individuals of the purposes of collection primarily through its program PIBs.

In such cases where the Department is collecting information about individuals indirectly, a reference to the appropriate PIB on forms and systems used for the indirect collection of data is expected by the *Privacy Act*. In addition, TBS expects the referenced PIBs to more completely describe the data elements being collected from program partners. Our review of the Department's PIB for FOAEA indicated that the PIB simply states that "identifying information" may be collected, without setting out the kinds or categories of identifying information being collected and used for program purposes. According to the TBS *Directive on Privacy Practices*, a privacy impact assessment (PIA) must be provided to TBS along with the substantially modified PIB description for registration and approval of the PIB.

Overall, while FLAS is meeting most of its obligations to identify the purposes for which it is collecting personal information, privacy notices as a whole should be improved to reflect the minimum content as stipulated in section 6.2.9 of the TBS *Directive on Privacy Practices*.

Privacy Impact Assessments

Section 4 of the *Privacy Act* requires the Department to limit its collection of personal information to that which is required for authorized operating activities. Sections 7 and 8 of the Act go on to restrict the use and disclosure of that information to the purposes for which it was first collected, except with the consent of the individual or as allowed by law. Finally, in order to protect the integrity of data, subsection 6(2) of the Act requires the Department to take all reasonable steps to ensure that personal information that is used for an administrative purpose is as accurate, up-to-date and complete as possible.

To ensure these requirements are met, departments generally establish operating and administrative controls. Departments are also required to perform periodic risk assessments in relation to key programs and activities. A PIA is one such risk process designed to mitigate potential privacy risks. It is the component of risk management that focuses on ensuring compliance with the *Privacy Act* requirements. PIAs are mandated under the TBS *Directive on Privacy Impact Assessment* for all new programs involving personal information, or where there are substantial modifications to existing programs or services involving personal information.

The audit noted that FLAS has not yet undertaken a program PIA in relation to the FOAEA program. FOAEA accounts for a large part of the unit's personal information holdings. The program was the subject of a formal PIA in 2010, however the review was limited to a review of impacts associated with changes to memoranda of understanding with TC and Passport Canada. In light of the substantial changes made within the program since its inception, we would have expected FLAS to have undertaken a PIA with respect to FOAEA's operations as a whole. FLAS management reported that a PIA for the FOAEA program as a whole has never been undertaken because the program was brought into force prior to the introduction of policy requirements governing PIAs. FLAS management recognizes the current need for a PIA because the outputs of the PIA would help meet its other policy obligations.

The inclusion and standardization of privacy notices are essential for compliance with TBS policy instruments. In addition, the absence of PIAs may adversely affect sound decision making by limiting careful consideration of privacy risks with respect to the creation, collection and handling of personal information as part of FLAS operations. Hence, the review of privacy notices and performing a PIA would further improve FLAS' sound privacy practices.

Recommendation 2	Management Action Plan
It is recommended that the Senior Assistant Deputy Minister, Policy Sector revise key policies supporting its obligations under the *Privacy Act* with a view to ensuring compliance with TBS directives by conducting the following: a. Initiate a program PIA for FOAEA where there is a substantial modification to its program activities, as per section 6.3.1 of the *Directive on Privacy Impact Assessment*; b. Review and revise all privacy notices on forms used for the collection of personal information, as per section	Management agrees with the recommendation. a. PIAs were completed in the past as required in accordance with the TBS *Directive on Privacy Impact Assessment*. A full PIA of the FOAEA program will be completed and its PIB updated. b. As indicated in the report, most collection of personal information of individuals is done indirectly in the performance of the administration of FLAS' programs. More specifically, personal information is received indirectly from applicants under the FOAEAA. Where the requirement exists, a privacy notice will be added to the applicable FOAEAA forms. Privacy notices have been

6.2.9 of the TBS *Directive on Privacy Practices*.	added to all other forms used in the administration of FLAS' programs.
Office of Primary Interest:	Senior Assistant Deputy Minister, Policy Sector
Due Date:	Privacy notices: o FOAEAA search request forms by June 30, 2017. o FOAEAA application forms by March 31, 2020. PIA for the FOAEA program: o Draft PIA for the FOAEA program to be completed by June 30, 2018. o Final PIA to be completed by the earliest of the following events: date that substantial modifications to the program's activities take place or March 31, 2020.

Manual Processing

The Department has made significant investments in IT to modernize its practices through the use of automation. As a result, FLAS has automated numerous processes to support the operations of FLAS and its client MEPs. For example, most of the FOAEA program's operational activities share information electronically with the provincial and territorial MEPs using either online applications or file transfer protocol. Despite the investments made in development of automated systems for the administration of key programs, there is still room for improvement in reducing the reliance on manual processing for select program tasks by further leveraging the Department's IT investments. This is particularly true with respect to the registration and processing of divorce proceedings under the CRDP, where only nine out of 185 courts across Canada are using direct online data entry systems. This reliance on manual processing increases the risk of data entry errors. Furthermore, manual processes are more costly and less efficient to operate. Although transitioning all partners towards automation may not be fully within FLAS' control, it would be beneficial for the Department to develop a plan that supports advancing the transition of key program operations to an automated process.

Recommendation 3	Management Action Plan
It is recommended that the Senior Assistant Deputy Minister, Policy Sector develop a work plan for the transition of CRDP core program functions and key program partners towards the direct and automated entry and processing of data.	Management agrees with the recommendation. With the objective of creating efficiencies and continuous improvement, management has made available to provincial/territorial partners various electronic means of exchanging information required under the CRDP Regulations. For example, it is working closely with its partners to provide secure external online access to its CRDP databank, where possible, to allow for direct input rather than paper forms. To date, 18 out of the 185 courts with which the CRDP transacts have online access. Management will continue during fiscal year 2017-18 its collaborative work with the various provincial/territorial officials to provide

	online access to additional courts. Where systems and technical resource capacity permit, other electronic options are being discussed to optimize efficiencies at a provincial level for all the courts within some jurisdictions. Any work plan developed will be subject to validation by provincial/territorial partners as to capacity to innovate further and allow for flexible delivery dates to accommodate provincial/territorial partners' competing priorities.
Office of Primary Interest:	Senior Assistant Deputy Minister, Policy Sector
Due Date:	Work plan to be completed by June 30, 2017.

7.3 Controls over the Integrity of Information

The audit examined the extent to which FLAS has designed IT general controls to support the integrity of data in the FOAEA system. In particular, we considered the extent to which FOAEA system data is transferred through the Department's network in accordance with its assigned security classification, and whether IT duties are segregated to minimize risk of errors and wrongdoing. Ensuring the integrity of data in the FOAEA system, the Department's only mission-critical system, is important to ensuring that the Minister is meeting statutory and policy obligations for program delivery.

Finding 3:

FLAS has designed controls to support the integrity of data in the FOAEA system. [redacted]

Linkage to: Controls

Network Security

Ensuring the security of information is paramount to the operation of the FOAEA program. Not only does the program handle and process a large volume of data, that data is mostly "personal information" which is information about identifiable individuals. In addition, FOAEA system data is also sensitive in nature as it relates to family orders and financial obligations arising from separation or divorce.

According to the Government of Canada's *Operational Security Standard: Management of Information Technology Security* (MITS), all federal departments must protect information throughout its life cycle in a manner commensurate with the information's sensitivity. Departments should encrypt Protected A and Protected B information, when supported by a threat and risk assessment (TRA). Furthermore, departments must:

- Encrypt Protected B information before transmitting it across the Internet or a wireless network;
- Use encryption or other safeguards endorsed or approved by the Communications Security Establishment (CSE).

While the recommendations of a recent draft TRA on the FOAEA system underscore the need for encryption in relation to FOAEA system Protected B data at rest, they do not address the unencrypted transmission of FOAEA system Protected B data (data in transit). Data encryption is an industry best practice that is employed to reduce the risk of unauthorized access. [redacted]

Recommendation 4	Management Action Plan
It is recommended that the Assistant Deputy Minister, Management and Chief Financial Officer Sector, complete the draft TRA on the FOAEA system and implement cryptographic safeguards to secure FOAEA system Protected B data, both at rest and in transit.	Management agrees with the recommendation. 1. The FOAEA system TRA recommendation #2 states "Adopt and implement CSE approved encryption for all FOAEA system data during [data at rest]." [redacted] The deadline below, as documented in the SIP, reflects various activities including but not limited to IT security review and approval of the selected encryption solution, technical and performance testing, and production implementation of the solution. 2. [redacted] The deadline below reflects various activities including but not limited to consultation with Shared Services Canada, IT security review and approval [redacted] technical and performance testing, and production implementation of the solution.
Office of Secondary Interest:	Assistant Deputy Minister, Management and Chief Financial Officer Sector
Due Date:	1. September 29, 2017 2. March 31, 2018

Segregation of Duties

Segregation of duties is a core concept of internal controls which constitutes separating conflicting sensitive tasks as a means to prevent error and wrongdoing. According to the MITS, departments must segregate IT responsibilities as much as reasonably possible to ensure that no single person has complete control of an entire IT system or a major operational function.

The Department's ISB appropriately segregated computer operations (e.g., infrastructure management, helpdesk and data entry) where each group is responsible for a distinct set of tasks. However, application development, testing and deployment duties, which should be segregated per industry standards, are all being performed by the application development team of the FOAEA system. These developers also have access to the FOAEA system database so as to perform database administration duties.

[redacted]

Recommendation 5	Management Action Plan
It is recommended that the Assistant Deputy Minister, Management and Chief Financial Officer Sector, segregate the roles, and associated duties, of application development, testing and deployment, and database administration, for the FOAEA system.	Management agrees with the recommendation. 1. ISB will define and document the duties, operational procedures and system access rights related to the roles of database administration, application development, application testing, and application deployment into production for the FOAEA system. 2. ISB will assign duties to personnel working on the FOAEA system and within teams designated to support the FOAEA system. [redacted] Prior to full implementation, ISB will conduct thorough testing of the system access rules. [redacted] but also ensure that duties can be carried out effectively within the parameters of the newly defined system access.
Office of Secondary Interest:	Assistant Deputy Minister, Management and Chief Financial Officer Sector
Due Date:	1. March 31, 2017 2. September 29, 2017

8. Opportunity – Government of Canada Open Data Initiative

In operating the FOAEA, CRDP and GAPDA programs, FLAS generates data on Canadian families that is of interest to a number of stakeholders including academics, researchers and policy groups. This data could also be useful to provinces and territories and their respective MEPs, allowing them to make more informed decisions about matters that affect families across Canada. At this time, the Department is not sharing FLAS data with these stakeholders.

In light of the Government of Canada's Open Data initiative, there is now an opportunity for the Department to revisit its policy on sharing aggregate data for research, statistical and policy purposes. It could explore the possibility of anonymizing and de-identifying data in order to share FLAS information both inside and outside of government to increase transparency while still respecting the privacy of individuals.

9. Audit Opinion

In my opinion, the Department has effective governance mechanisms in place to support the administration of the CRDP, FOAEA and GAPDA programs. Privacy controls are designed to help ensure the proper[5] handling of personal information, and overall, the Department is meeting its obligations under the *Privacy Act* with respect to the handling of personal information by FLAS. Controls are designed to support the integrity of information and data in the FOAEA system such that FLAS is meeting its obligations under the FOAEAA. Opportunities for improvement to further mitigate risks exist and management has demonstrated a strong commitment and proactive approach to making improvements as issues arise.

[5] 'Proper' in this context means the handling of personal information in compliance with sections 4 through 8 of the *Privacy Act*, and in a manner that is appropriate in the circumstances.

Appendix A – Audit Criteria

Line of Enquiry 1 – GOVERNANCE

Criterion 1.1 – Governance mechanisms are in place to support the administration of the CRDP, FOAEA and GAPDA programs.

1.1.1 The organization has plans in place aimed at achieving its strategic objectives.

1.1.2 Management has identified and tracked performance measures and service standards linked to strategic objectives.

1.1.3 Roles and responsibilities are defined, communicated and assigned to functional experts where applicable.

1.1.4 Memoranda of understanding, or equivalent, outline terms and conditions for the proper handling of personal information and the roles and responsibilities of the Department and other partner organizations.

Line of Enquiry 2 – INTERNAL CONTROLS

Criterion 2.1 – The FLAS unit has designed controls to help ensure the proper[6] handling of personal information.

2.1.1 Processes are in place to inform individuals whose personal information is being collected of the purposes of that collection (except as provided by law).

2.1.2 Controls are in place to limit the collection, use, disclosure and retention of personal information to that which is provided by law.

2.1.3 Controls are in place to help ensure the accuracy and completeness of personal information used to make administrative decisions about an individual.

2.1.4 Controls are in place to safeguard personal information under the FLAS unit's control from unauthorized uses or disclosures.

Criterion 2.2 – The FLAS unit has designed controls to support the integrity of information and data in the FOAEA system.

2.2.1 Key information technology duties[7] are segregated to minimize the risk of errors and wrongdoing.

2.2.2 FOAEA system data is transferred through the Department's network in accordance with the security classification requirements of FOAEA system data.

2.2.3 User input modifications to the financial terms of garnishments in the FOAEA system are monitored to validate the accuracy of the changes.

[6] 'Proper' in this context means the administration of programs and data in compliance with governing law and regulations, and in a manner that is suitable in the circumstances.

[7] Key duties include system development, testing, deployment, security, maintenance, database administration and information technology support.