Q & A Guidelines for Government Employees and Contractors:

Assessing Government Contracts for Compliance with the Privacy Provisions of the *Freedom of Information and Protection of Privacy Act*

(March 2005)

1. Does the contract involve personal information?

Personal information is defined in the *FOIPP Act* as "identifiable information about an individual other than contact information." Contact information includes the name, title, telephone or facsimile number, email address, etc., which enable an individual at a place of business to be contacted.

If the contract does **not** collect, use, disclose, or store personal information, then the privacy provisions of the *FOIPP Act* do not apply to the contract.

2. If the contract does involve personal information, what kind of personal information is it?

Different types of personal information can have varying degrees of sensitivity and this can determine how it should be handled and what level of protection or precaution is required. Also, the sensitivity of certain personal information can vary in different circumstances. For example, an individual's home address may or may not be particularly sensitive information depending on the situation or its use, whereas an individual's health information is almost always sensitive.

You should review and evaluate the kind of personal information that the contract will involve. To minimize the privacy impact of the contract, you may want to consider reducing or eliminating the involvement of personal information that is not essential for the service provider to have or handle.

3. Will the service provider be collecting, using, disclosing, or storing the personal information?

If a service provider will **in any way** collect, use, disclose, or store personal information as part of its services under the contract, then the service provider is subject to the terms and conditions of the privacy provisions of the *FOIPP Act*. If the service provider will not directly collect, use, disclose or store

personal information, but will have access to it, then the service provider is still subject to the privacy provisions of the *FOIPP Act*.

You must ensure that the contract states that the service provider is subject to the provisions of the *FOIPP Act* and attach the Privacy Protection Schedule to the contract.

4. Will the service provider be subcontracting any of its services?

If the service provider will be subcontracting some of its work or services to another service provider, then the contract must state that the subcontractor(s) is also subject to the provisions of the *FOIPP Act* and to the Privacy Protection Schedule.

Additionally, the contract should include specific "flow-through" provisions that require subcontractors to adhere to the same specific privacy and security terms agreed to by the primary contractor or that clarify where the terms may vary. For example, if the subcontractor will not have, nor need, access to the personal information involved in the contract, then this is an important provision to include in the contract.

The contract should also address the issue of changes or additions to subcontractors, such as whether new subcontractors are permissible under the contract and whether government must approve them first. Secondly, it should be clear in the contract that if additional or alternate subcontractors are hired, they must adhere to the provisions of the *FOIPP Act* as set out in the Privacy Protection Schedule or any other addenda.

5. Is the personal information physically located outside of Canada or will it be?

Section 30.1 of the *FOIPP Act* requires all personal information in the custody or under the control of government and its service providers to be **stored and accessed only in Canada**. This general rule applies **unless** the individual the information is about consents to it being stored or accessed from another jurisdiction, or where the *FOIPP Act* specifically allows disclosure to a foreign jurisdiction for one of the purposes set out in section 33.1. For example, personal information may be disclosed outside of Canada for the purposes of collecting monies owed to the BC government or so the next of kin or a friend of an injured, ill or deceased individual may be contacted.

You should carefully review how and where the personal information involved in the contract is, or will be, stored and accessed, and what uses, including disclosures, of the information by service providers and subcontractors may

be involved. You may need to include some specific provisions in the contract that address these issues, so that it is clear who has access to what, where, when and how.

6. What are your security arrangements for protecting personal information?

The *FOIPP Act* requires government to make reasonable security arrangements against such risks as unauthorized access, use, disclosure or disposal of personal information. This includes both physical and electronic risks and pertains to service providers and subcontractors as well as government itself. These security arrangements should form an essential part of the contract.

You should review the existing or planned security arrangements for the personal information involved in the contract to identify or develop:

- Reasonable technical security arrangements;
- Reasonable physical security arrangements;
- Specific security policies and procedures;
- A "need-to-know" basis for users regarding access rights to personal information;
- Specific administrative controls and procedures for the authority to add, change or delete personal information;
- A regularized audit process that can track use of the personal information, such as who accessed and or updated the system, when, and how so that inappropriate accesses to the system can be identified.

7. How do you determine whether a company is Canadian or has American affiliation?

The following points are the best earmarks of BC or Canadian origin or status:

- Search the BC company registry to see if the company is incorporated in BC. A company must be incorporated in BC in order to operate in BC. Search the federal registry to see if the company is incorporated in Canada.
- Look at the company's Charter and Articles of incorporation for more information about the company.
- Look at the location of the company's office. A company must have an office in BC to be a BC company or elsewhere in Canada to be a Canadian company.

- Look at where the company keeps its records. A company must keep its records in a BC office if it is a BC company or elsewhere in Canada if it is a Canadian company.
- Look at the residency of the company's directors. The majority of directors must reside in BC or Canada if it is a BC or Canadian company.
- Look at the location of the company's general meetings. A company's general meetings must be held in BC if it is a BC company or authorized by the registrar to be held elsewhere if it is a Canadian company.