THE SECURITY OF INFORMATION?

The Government Security Policy establishes a framework of policy guidelines for implementing information security and privacy requirements. This framework requires the Department to properly safeguard personal information and other sensitive data contained in its information systems or used in its programs and services. The policy is based on the principle that safeguards for information and assets should clearly reflect their sensitivity, importance and value—no more and no less.

Your responsibility is to protect the sensitive information and assets that you handle on a day-to-day basis. This means protecting it against unauthorized disclosure, destruction, removal or modification. No one wants to compromise any information that could endanger the national interest or other interests for which Parliament assumes an obligation.

In your day-to-day work, make sure that you can:

- ✔ identify information that is sensitive;
- ✔ choose the appropriate level of sensitivity for information you create, and,
- ✔ mark this information correctly so others see the need for special protection.

You should also be able to:

- ✔ select secure equipment and a secure location to write, discuss and transmit information;
- ✔ store information securely; and
- ✔ destroy the information safely and securely.

WHAT IS SENSITIVE INFORMATION?

Not all information needs to be classified or designated. However, at a minimum, departmental information and assets should receive a level of reasonable care that is consistent with basic administrative practices. Certainly, information should never be classified nor designated to conceal violations of the law, inefficiencies or administrative errors, nor to avoid embarrassment or to restrain competition.

It is true, however, that some information and certain assets are more sensitive or valuable than others and therefore, require more stringent safeguards. In line with