developed for all domestic facilities, and work is being done on them at the Missions abroad

- Building condition report assessments are conducted regularly
- Security clearances are sought wherever possible
- Incident reporting is strongly urged

A Memorandum to Cabinet (MC) has been submitted in December 2006 to request increased funding for security.

The IT renewal initiative addresses IT security, and Management of Information Technology Security (MITS) implementation is beginning within DFAIT. Departmental policies such as the Network Use Agreement and the Conduct Abroad Code are endorsed by staff.

Partners such as the RCMP and CSIS supply information to DFAIT, and intelligence is shared amongst allies. Media analyses are conducted regularly within the Department for intelligence gathering purposes.

Contingency Planning initiatives underway include:

- Standard Operating Procedures for some situations have been developed, and staff training and awareness of security issues is ongoing
- Some branches have in place duty rosters for after-hours service or response for security and IT Systems

The Public Sector Disclosure Act and other guidelines include measures to protect safety and security.

DFAIT has a cultural readiness to accept risk and staff generally demonstrates a willingness to take on higher-risk assignments.

Potential Impacts

If this risk were to materialize, it could diminish the health and safety of individuals or result in injury or loss of life. From an asset perspective, sensitive information may be lost or stolen.

Productivity, effectiveness, and quality of services would be reduced as staff respond to incidents. There is also the potential for mission closures and staff reluctance to take on more dangerous assignments can result in the inability to provide