INFORMATION SHARING AND PROTECTION
UNDER THE EMERGENCY MANAGEMENT ACT

Critical Infrastructure Policy

Emergency Management and National Security Branch

December 2007

Public Safety Canada
Sécurité publique Canada

Canada

Table of Contents

Introduction

One of the key principles behind the *Emergency Management Act (EMA)* is that critical infrastructure protection (CIP) is an integral part of modern emergency management. Public Safety Canada's responsibilities under both the *EMA* and the *Department of Public Safety and Emergency Preparedness Act*, include facilitating the sharing of information to strengthen emergency preparedness and public safety.

The ability to exchange specific and reliable information in a timely manner with the private sector is essential to the government's role in providing national leadership in emergency management and CIP. Assessing threats and vulnerabilities, improving warning and reporting capabilities, analyzing attacks to develop better defences and responses, are the primary goals of information sharing under the *EMA*.

Timely information provided by the private sector will enable better understanding of CI sector interdependencies and the state of preparedness in CI sectors. It will also enable the government to better adjust national plans, promote risk reduction measures and enhance resiliency in Canada's CI. It will enable the government to improve its capability to provide more useful information products to its stakeholders. During emergency situations, effective information exchange among CI partners is essential for accurate situational awareness and efficient and effective operational response.

The *EMA* includes a consequential amendment to the *Access to Information Act* that allows the Government of Canada to protect specific critical infrastructure information supplied in confidence to the government by third parties. Private sector partners should note that critical infrastructure information can be protected under this exemption only if it is appropriately marked and is treated as confidential by the entity that provides the information. It should also be noted that exemptions from disclosure for reasons of national security and public safety already exist under federal/provincial/territorial access to and freedom of information legislation.

The end result of these efforts to promote information sharing will be the development of a more coherent approach to emergency management at the national level and thereby ensure the maximum utility of the *EMA*.

The following information is a more detailed guide to the consequential amendment to the *Access to Information Act* pursuant to the *EMA*.

Guide to *Access to Information Act* (*ATIA*) paragraph 20(1)(b.1)

1. What is paragraph 20(1)(b.1)?

- Subsection 20(1) of the *Access to Information Act* is amended by adding the following provision after paragraph (b):

  (b.1) "information that is supplied in confidence to a government institution by a third party for the preparation, maintenance, testing or implementation by the government institution of emergency management plans within the meaning of section 2 of the *Emergency Management Act* and that concerns the vulnerability of the third party's buildings or other structures, its networks or systems, including its computer or communications networks or systems, or the methods used to protect any of those buildings, structures, networks or systems "

- This is a mandatory exemption ("*the head of a government institution* ***shall*** *refuse to disclose any record requested under this Act that contains* […]"). This means that the information must not be disclosed, unless conditions specified in the *ATIA* are met. These include:
  - the third party consented to the disclosure; or
  - the information constitutes results of product or environmental testing carried out by the government for the third party at no cost; or
  - the disclosure would be in the public interest as it relates to public health, public safety or protection of the environment.

- Government institutions must consult third parties when a request has been received under the *ATIA* and the institution intends to disclose records that contain or may contain third party information (see question #11 and Annex 1 for more details).

2. Why is paragraph 20(1)(b .1) necessary as a consequential amendment under the *Emergency Management Act* (*EMA*)?

- The ability to rapidly exchange specific and reliable information in a timely manner with the private sector is essential to the Government's role in providing national leadership in emergency management and critical infrastructure protection. Assessing threats and vulnerabilities, improving warning and reporting capabilities, analyzing attacks to develop better defenses and responses, are the primary goals of information sharing under the *EMA*.

- The intent of this exemption is to enhance information sharing between the Government of Canada (GC) and the private sector. As the private sector owns or operates over 85% of Canada's critical infrastructure (CI), such information is necessary to obtain an accurate picture of the state of CI resilience in Canada.

- The GC is not in a position to compel the private sector to share sensitive critical infrastructure/emergency management (CI/EM) information by regulation or other legislated means because Canada's CI sectors operate in a complex regulatory environment governed by multiple jurisdictions. The GC therefore promotes voluntary information sharing mechanisms with the private sector.

- CI/EM information is, by its nature, highly sensitive. Consequently, prudent CI/EM owners/operators take appropriate action to ensure that this information remains confidential. This exemption is required to remove any doubt as to whether such information will be protected if they choose to share it with the GC. Inappropriate release of such information could potentially cause harm to CI owners/operators by putting the security of their physical and cyber infrastructure at risk

3. When does paragraph 20(1)(b.1) apply?

- As all other exemptions, when there is a formal request under the *ATIA.*

- When the requested record is under the control of a government institution, i.e., when the institution has legal or physical possession of the record.

4. What criteria have to be met in order to apply this exemption?

- The information must meet the following conditions to qualify for this exemption:

  - The information is provided for the preparation, maintenance, testing or implementation by the government institution of emergency management plans within the meaning of section 2 of the *Emergency Management Act* and for uses consistent with this purpose.

  - The information must be about the vulnerability of the third party's buildings or other structures, its networks or systems, including its computer or communication networks or systems, or the methods to protect any of these. No other type of information is covered by this exemption, although other provisions of the *ATIA* may apply.

- The record must be provided in confidence to the Government of Canada by the third party. In order to indicate confidentiality, the third party should mark its record prior to transmittal (see question #5).

- The information must be consistently treated as confidential by the third party (prior to, during and after transmittal).

5. Will records provided in confidence to the Government by a third party automatically be exempted?

- A designation of confidentiality does not of itself ensure that the information is automatically exempt from access. In the event of an *ATIA* request, the information will still have to be examined on a case by case basis to determine if it qualifies as information provided in confidence and if it meets the other criteria of the exemption.

- This examination will entail an assessment of the markings or transmittal documents to determine whether the information was provided to the Government in confidence, whether it was consistently treated in a confidential manner by the third party and whether it was provided for the purpose of preparing, maintaining, testing or implementing emergency management plans by the Government institution to which it was submitted.

- The information itself must be examined to determine whether it concerns the vulnerability of the third party's buildings or other structures, its networks or systems, including its computer systems or communications networks or systems, or the methods used to protect any of those buildings, structures, networks or systems.

- If there is uncertainty about the nature or the confidentiality of the information, the institution will consult the third party who provided the information to determine if it falls under paragraph 20(1)(b.1) or another paragraph of section 20, if the information is still confidential, and if the third party consents to its disclosure.

- Third party consent must be obtained by government institutions in writing, either at the time of submission, during informal consultation or in response to the notification of the intent to disclose by the government institution required by section 27 of the *ATIA*.

- See question # 11 and Annex 1 for additional information on third party intervention

6. What are some examples of CI/EM information to be covered by this exemption?

- Examples could include, but not necessarily be limited to:

  - vulnerability/risk assessments of critical cyber and physical infrastructure systems and networks
  - assessments of potential consequences of CI failures or disruptions, both physical and cyber
  - methods/protocols for prevention/mitigation, preparedness, response and recovery to CI vulnerabilities, disruptions or incidents
  - plans/analyses addressing CI interdependencies
  - key elements of service continuity or business resumption plans, such as special arrangements for obtaining emergency supplies to continue essential operations, alternate locations for critical operations or redundant systems, internal emergency communications protocols, etc.
  - maps/plans of critical assets, facilities, installations, communications nodes, computer networks, etc.
  - sensitive information on CI protection activities and response plans
  - defence measures to counter malicious cyber intrusions or attacks
  - techniques/protocols to protect SCADA systems
  - CI/EM information that, if it were to fall into the wrong hands, could be exploited to debilitate an organization in its recovery from a CI failure, attack or disruption
  - information that would identify the entity that supplied the information in confidence, as well as the entity on whose behalf the information has been provided.

7. Could other *ATIA* exemptions be used to protect this type of information in addition to paragraph 20(1)(b.1)?

- Depending on the nature of the information in question, it is possible that other exemptions could apply to CI/EM information.

- See Annex 2 for an outline of the other exemptions in the *ATIA*.

- Please note that the exclusions under the *ATIA* (sections 68, 68.1, 68.2 and 69) are not addressed in this document.

8. Does the principle of severability (section 25) apply to information qualifying for this exemption?

- Once it has been determined that a record qualifies for this exemption, consideration is required whether any part of the material can reasonably be severed.

- Reasonable severance is accomplished where a document with deletions remains meaningful and there has been no distortion in the meaning of the original text.

- Severance that results in the disclosure of disconnected snippets of information is not reasonable because what is disclosed may be meaningless or misleading as the information it contains is taken out of context, or may provide clues to the contents of the deleted portions.

- As there will be considerable variation in the form and content of CI/EM information submitted to government institutions, the determination of severability will need to be made on a case-by-case basis. Examples of information to be severed could include identification of alternate locations for essential services, locations of stockpiles of vaccines and other emergency supplies, among others (see question # 6 for additional examples).

9. Can this process be used to collect personal information and potentially infringe on the privacy of Canadians?

- There is no intention to collect personal information as part of this exercise.

- If an activity of the Government of Canada requires the collection or the sharing of personal information, the Privacy Act and any other relevant legislation will be applied to the government activity.

10. Could paragraph 20(1)(b.1) conceal from the public the failure of private sector companies to adequately identify their vulnerabilities, take action to protect their infrastructure or pollute the environment?

- It is recognized that there will be instances where it will be important to disclose this type of information in the public interest. This is the purpose of the public interest override in subsection 20(6). This discretionary provision requires the head of a government institution to exercise discretion in balancing competing public interest, that is, protecting the interests of third parties versus disclosing the information because of a greater public interest. However, subsection 20(6) does not apply to trade secrets.

- Wording has been added to subsection 20(6) to explicitly recognize that the information may be disclosed in whole or in part if the disclosure would be in the public interest as it relates to public health, public safety or the protection of the environment and, if the public interest in disclosure clearly outweighs in importance any financial loss or gain to a third party, any prejudice to the security of its structures, networks or systems, any prejudice to its competitive position or any interference with its contractual or other negotiations.

- Requesters can complain to the Information Commissioner (IC) for arm's length investigation of a refusal to disclose information and obtain a non-binding recommendation.

- If not satisfied by the IC's recommendation, or if the government institution continues to deny access to the record, the requester can apply to the Federal Court for review and a binding order.

- The IC has access to any record to which the Act applies in connection with a complaint investigation, and no such record may be withheld on any grounds.

- In litigation, disclosure of documents follows the rules of the Court

11. Will third parties have a say as to whether the information they provided will be disclosed under the *Access to Information Act*?

- The Act contains several provisions that permit third parties to intervene during the processing of the request, the investigation of a complaint and a review by the Federal Court.

- During the processing of the request:

  - The third party is given an opportunity to make written representations when a government institution intends to disclose records that contain or may contain third party information (paragraph 28(1)(a)).

  - The third party may apply to the Federal Court for a review of the decision of the institution (section 44).

- During the investigation of a complaint:

  - The third party is given an opportunity to make representations to the Information Commissioner (subsection 35(2)).

  - The Information Commissioner reports the result of the investigation to the third party that made representations (subsection 37(2)).

- If the government institution decides, on the recommendation of the Information Commissioner, to disclose the records, it gives notice of the decision to the third party (section 29).

- The third party may apply to the Federal Court for a review of the decision of the institution (section 44).

- <u>During a review by the Court:</u>

  - If the requester or the Information Commissioner applies to the Federal Court for a review of the decision of the institution not to disclose the information, the institution must advise the third party (subsection 43(1).

  - The third party may appear as a party to the review (subsection 43(2)).

ANNEX 1 Provisions of the Access to Information Act Related to Third Party Intervention

Notice to third parties

27. (1) Where the head of a government institution intends to disclose any record requested under this Act, or any part thereof, that contains or that the head of the institution has reason to believe might contain

(a) trade secrets of a third party,

(b) information described in paragraph 20(1)(b) or (b.1) that was supplied by a third party, or

(c) information the disclosure of which the head of the institution could reasonably foresee might effect a result described in paragraph 20(1)(c) or (d) in respect of a third party,

the head of the institution shall, subject to subsection (2), if the third party can reasonably be located, within thirty days after the request is received, give written notice to the third party of the request and of the fact that the head of the institution intends to disclose the record or part thereof.

Waiver of notice

(2) Any third party to whom a notice is required to be given under subsection (1) in respect of an intended disclosure may waive the requirement, and where the third party has consented to the disclosure the third party shall be deemed to have waived the requirement.

Contents of notice

(3) A notice given under subsection (1) shall include

(a) a statement that the head of the government institution giving the notice intends to release a record or a part thereof that might contain material or information described in subsection (1);

(b) a description of the contents of the record or part thereof that, as the case may be, belong to, were supplied by or relate to the third party to whom the notice is given; and

(c) a statement that the third party may, within twenty days after the notice is given, make representations to the head of the government institution that

has control of the record as to why the record or part thereof should not be disclosed.

Extension of time limit

(4) The head of a government institution may extend the time limit set out in subsection (1) in respect of a request under this Act where the time limit set out in section 7 is extended under paragraph 9(1)(a) or (b) in respect of the same request, but any extension under this subsection shall be for a period no longer than the period of the extension under section 9.

Representations of third party and decision

28. (1) Where a notice is given by the head of a government institution under subsection 27(1) to a third party in respect of a record or a part thereof,

(a) the third party shall, within twenty days after the notice is given, be given the opportunity to make representations to the head of the institution as to why the record or the part thereof should not be disclosed; and

(b) the head of the institution shall, within thirty days after the notice is given, if the third party has been given an opportunity to make representations under paragraph (a), make a decision as to whether or not to disclose the record or the part thereof and give written notice of the decision to the third party.

Representations to be made in writing

(2) Representations made by a third party under paragraph (1)(a) shall be made in writing unless the head of the government institution concerned waives that requirement, in which case they may be made orally.

Contents of notice of decision to disclose

(3) A notice given under paragraph (1)(b) of a decision to disclose a record requested under this Act or a part thereof shall include

(a) a statement that the third party to whom the notice is given is entitled to request a review of the decision under section 44 within twenty days after the notice is given; and

(b) a statement that the person who requested access to the record will be given access thereto or to the part thereof unless, within twenty days after the notice is given, a review of the decision is requested under section 44.

Disclosure of record

(4) Where, pursuant to paragraph (1)(b), the head of a government institution decides to disclose a record requested under this Act or a part thereof, the head of the institution shall give the person who made the request access to the record or the part thereof forthwith on completion of twenty days after a notice is given under that paragraph, unless a review of the decision is requested under section 44.

Where the Information Commissioner recommends disclosure

29. (1) Where the head of a government institution decides, on the recommendation of the Information Commissioner made pursuant to subsection 37(1), to disclose a record requested under this Act or a part thereof, the head of the institution shall give written notice of the decision to

(a) the person who requested access to the record; and

(b) any third party that the head of the institution has notified under subsection 27(1) in respect of the request or would have notified under that subsection if the head of the institution had at the time of the request intended to disclose the record or part thereof.

Contents of notice

(2) A notice given under subsection (1) shall include

(a) a statement that any third party referred to in paragraph (1)(b) is entitled to request a review of the decision under section 44 within twenty days after the notice is given; and

(b) a statement that the person who requested access to the record will be given access thereto unless, within twenty days after the notice is given, a review of the decision is requested under section 44.

Notice to third parties

33. Where the head of a government institution refuses to disclose a record requested under this Act or a part thereof and receives a notice under section 32 of a complaint in respect of the refusal, the head of the institution shall forthwith advise the Information Commissioner of any third party that the head of the institution has notified under subsection 27(1) in respect of the request or would have notified under that subsection if the head of the institution had intended to disclose the record or part thereof.

Right to make representations

35. (2) In the course of an investigation of a complaint under this Act by the Information Commissioner, a reasonable opportunity to make representations shall be given to

(a) the person who made the complaint,

(b) the head of the government institution concerned, and

(c) where the Information Commissioner intends to recommend under subsection 37(1) that a record or a part thereof be disclosed that contains or that the Information Commissioner has reason to believe might contain

(i) trade secrets of a third party,

(ii) information described in paragraph 20(1)(b) or (b.1) that was supplied by a third party, or

(iii) information the disclosure of which the Information Commissioner could reasonably foresee might effect a result described in paragraph 20(1)(c) or (d) in respect of a third party,

the third party, if the third party can reasonably be located,

but no one is entitled as of right to be present during, to have access to or to comment on representations made to the Commissioner by any other person.

Notice to third parties

43. (1) The head of a government institution who has refused to give access to a record requested under this Act or a part thereof shall forthwith on being given notice of any application made under section 41 or 42 give written notice of the application to any third party that the head of the institution has notified under subsection 27(1) in respect of the request or would have notified under that subsection if the head of the institution had intended to disclose the record or part thereof.

Third party may appear as party

(2) Any third party that has been given notice of an application for a review under subsection (1) may appear as a party to the review.

Third party may apply for a review

44. (1) Any third party to whom the head of a government institution is required under paragraph 28(1)(b) or subsection 29(1) to give a notice of a decision to disclose a record or a part thereof under this Act may, within twenty days after the notice is given, apply to the Court for a review of the matter.

ANNEX 2 Exemption Provisions of the *Access to Information Act*

The following lists the provisions of the *Access to Information Act* that allow government institutions to refuse to disclose information subject to the Act that is under their control. For additional information on these provisions, please consult the *Access to Information Act* or the Treasury Board's Access to Information Policy and guidelines.

13 - Information obtained in confidence from other governments

14 - Federal-provincial affairs

15 - International affairs and defence

16 - Law enforcement and investigations

16.1 - Investigations, examinations and audits of the Auditor General of Canada, the Commissioner of Offical Languages, the Information Commissioner and the Privacy Commissioner

16.2 - Investigations by the Commissioner of Lobbying

16.3 - Investigations, examinations and reviews under the Canada Elections Act

16.4 - Investigations by the Public Sector Integrity Commissioner

16.5 - Information related to disclosures and investigations under the Public Servants Disclosure Protection Act

17 - Safety of individuals

18 - Economic interests of Canada

18.1 - Economic interests of the Canada Post Corporation, Export Development Canada, the Public Sector Pension Investment Board and Via Rail Canada Inc.

19 - Personal information

20 - Third party information

20.1 - Information relating to investment obtained in confidence from a third party by the Public Sector Pension Investment Board

20.2 - Information relating to investment obtained in confidence from a third party by the Canada Pension Plan Investment Board

20.4 - Terms of a contract for the services of a performing artist or identity of a confidential donor of the National Arts Centre Corporation

21 - Operations of Government

22 - Testing procedures, tests and audits

22.1 - Internal audits

23 - Solicitor-client privilege

24 - Statutory prohibitions against disclosure

26 - Refusal of access where information to be published