IDENTIFYING AND MARKING CRITICAL INFRASTRUCTURE /EMERGENCY MANAGEMENT (CI/EM) INFORMATION SHARED IN CONFIDENCE WITH THE GOVERNMENT OF CANADA

GUIDE FOR PRIVATE SECTOR ENTITIES

1. Introduction

Unauthorized access to sensitive information about Canada's critical infrastructure can prove damaging to the private sector entities that share this information with the Government of Canada. For this reason, the *Emergency Management Act (EMA)* includes a consequential amendment to the *Access to Information Act (ATIA)* that allows the Government of Canada to protect from disclosure specific critical infrastructure / emergency management (CI/EM) information supplied in confidence to the government by third parties.

Private sector entities should note that the information they share in confidence with government institutions can be protected under the exemption for CI/EM information only if it is identified as such and appropriately marked by the third party that provides the information.

For more detailed information about the consequential amendment to the *Access to Information Act* to protect CI/EM information (i.e., paragraph 20(1)(b.1), please consult the publication *Information Sharing and Protection under the Emergency Management Act*. This is available from Critical Infrastructure Policy, Public Safety Canada.

The purpose of this Guide is to provide general guidance for private sector entities to help them identify sensitive CI/EM information and develop specific markings for this information when it is shared in confidence with the Government of Canada.

2. Applicability

The information in this Guide is applicable to private sector entities who voluntarily share in confidence specific critical infrastructure/emergency management information with Government of Canada departments and agencies.

3. Criteria the information must meet

To qualify for the exemption for CI/EM information in the *Access to Information Act, i.e.,* paragraph 20(1)(b.1):

- **The information must be supplied in confidence to a federal government institution by a third party;**

- The information must be supplied 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

- The information must concern 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.

4. Marking CI/EM information provided in confidence to the Government of Canada

In order to indicate that the information is being provided in confidence, the third party should mark **each page** of the document(s) prior to transmittal. Adherence to standard marking will help ensure that the information is protected consistently by federal government institutions who receive such information from their private sector critical infrastructure partners.

Once a document is identified as containing CI/EM information provided in confidence to a federal government institution, it should be marked according to the following:

PROTECTED
CRITICAL INFRASTRUCTURE / EMERGENCY MANAGEMENT INFORMATION
PROVIDED IN CONFIDENCE TO
[*name of federal department or agency*]

The marking shown above (frame and format optional) should be placed on all pages or sections of the document that contain CI/EM information. A stamp or label may be used.

The marking should be located either at the top or bottom of each page consistently throughout the document.

The size, format and arrangement of the words may be modified to accommodate different situations but the wording should remain consistent.

The marking should also appear on the outside of any front or back cover, any binder cover or folder (front and back) and any title page.

5. Identifying specific CI/EM information shared in confidence

Private sector entities should review the documents they share in confidence with the Government of Canada to determine if the subject matter concerns the first of the criteria outlined above.

Some points to consider when determining what constitutes CI/EM information to be shared in confidence:

- What impact could the information have if it was inadvertently transferred to an unintended audience?
- Does the information provide details concerning critical infrastructure vulnerabilities, security procedures and capabilities or protective measures?
- Could someone use the information to target personnel, facilities, structures, systems, networks or operations?
- Could someone intent on causing harm misuse the information?
- Could the use of this information be dangerous if combined with other publicly available information?
- Is the information customarily public knowledge? Information that is accessible to the general public if there has been no deliberate attempt to keep it confidential or secret, or if it is posted to a public website, does not qualify for the exemption for CI/EM information, i.e., *ATIA* paragraph 20(1)(b.1) would not apply.

Examples of CI/EM information shared in confidence could include but not 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 process control, also known as SCADA, systems;
- CI/EM information that, if it were to be accessed by unauthorized parties, could be exploited to cause harm to an organization's critical services or debilitate it in its recovery from a CI failure, attack or disruption; or
- information that would identify the entity that provided the information, as well as the entity on whose behalf the information has been provided.

6. List of *Access to Information Act* exemptions

The following is a list of exemptions in the *Access to Information Act (ATIA)* that allow government institutions to refuse to disclose information that is under their control. For more detailed information about these exemptions please consult the *ATIA* (available on-line at www.infocom.gc.ca) or your legal counsel.

13 - Information obtained in confidence from other governments

14 - Federal-provincial affairs

15 - International affairs and defence

16 - Law enforcement and investigations, including 16(2)(c) on the vulnerability of particular buildings or other structures or systems …

16.1 - Investigations, examinations and audits of the Auditor General of Canada, the Commissioner of Official 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, including 20(1)(b.1) for CI/EM information supplied in confidence …

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 is to be published

7. Purpose of sharing CI/EM information with the Government of Canada

Sharing CI/EM information between the federal government and 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 defences and responses, are the primary goals of sharing CI/EM information under the authority of the *EMA*.

8. Transmitting CI/EM information shared in confidence with the Government of Canada

CI/EM information provided in confidence to the Government of Canada should be transmitted in hard copy by secure, trackable methods such as express, certified or registered mail or commercial courier service. In electronic format, the information should be transmitted in a protected format, such as a locked PDF file or password protected document with the password provided under separate cover, or using an encryption method agreed upon with the information sharing partner.

9. Contact information

For additional information about any aspect of this Guide, please contact:

Director
Critical Infrastructure Policy
Public Safety Canada
269 Laurier Avenue West
Ottawa, Ontario
Canada K1A 0P8

(613) 991-3583