



**AUDIT OF THE JUSTICE CANADA
EMERGENCY MANAGEMENT PROGRAM
AND THE BUSINESS CONTINUITY PLANNING PROGRAM**

**May 3, 2013
Internal Audit Branch**

AUDIT OF THE JUSTICE CANADA EMERGENCY MANAGEMENT PROGRAM AND THE BUSINESS CONTINUITY PLANNING PROGRAM

- Information contained in this publication or product may be reproduced, in part or in whole, and by any means, for personal or public non-commercial purposes, without charge or further permission, unless otherwise specified.
- You are asked to:
 - exercise due diligence in ensuring the accuracy of the materials reproduced;
 - indicate both the complete title of the materials reproduced, as well as the author organization; and
 - indicate that the reproduction is a copy of an official work that is published by the Government of Canada and that the reproduction has not been produced in affiliation with, or with the endorsement of the Government of Canada.
- Commercial reproduction and distribution is prohibited except with written permission from the Department of Justice Canada. For more information, please contact the Department of Justice Canada at: www.justice.gc.ca.

©Her Majesty the Queen in Right of Canada,
represented by the Minister of Justice and Attorney General of Canada, 2013

ISBN 978-1-100-22897-6

Cat. No. J2-387/2013E-PDF

TABLE OF CONTENTS

STATEMENT OF CONFORMANCE AND ASSURANCE..... i

EXECUTIVE SUMMARY ii

1.0 INTRODUCTION 1

 1.1 Background 1

 1.4 Audit Criteria..... 3

 1.6 Identified Strengths 4

2.0 FINDINGS, RECOMMENDATIONS AND MANAGEMENT RESPONSES 5

3.0 AUDIT OPINION/OVERALL CONCLUSION 11

APPENDIX A - STANDARDS/REFERENCES 12

APPENDIX B - EM AND BCP GOVERNANCE STRUCTURE..... 13

APPENDIX C – EM EXERCISES/EVENTS 14

APPENDIX D – BCP EXERCISES 15

APPENDIX E - JUSTICE EMERGENCY OPERATIONS CENTER 16

APPENDIX F – AUDIT CRITERIA..... 18

APPENDIX G – APPROACH AND METHODOLOGY 19

APPENDIX H – CORPORATE BCPs – OUTDATED &/OR MISSING ELEMENTS 21

APPENDIX I – REGION BCPs – OUTDATED &/OR MISSSING ELEMENTS 22

APPENDIX J – RISK ASSESSMENT GUIDELINES 23

APPENDIX K – ACRONYMNS/ABBREVIATIONS 24

APPENDIX L – INTERVIEWS/MEETINGS BY POSITION 26

STATEMENT OF CONFORMANCE AND ASSURANCE

We have completed the internal audit of the Emergency Management program and the Business Continuity Planning program at the Department of Justice. The overall objective of the audit was to provide assurance that the management control framework is effective for these programs.

This audit conforms to the Internal Auditing Standards for the Government of Canada, as supported by the results of the quality assurance and improvement program.

In our professional judgment, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the conclusion provided and contained in this report.

The conclusion is based on a comparison of the conditions, as they existed at the time of the audit, against pre-established audit criteria that were derived from the OCG publication *Audit Criteria Related to the Management Accountability Framework: A Tool for Internal Auditors* (OCG, March 2011).

Original signed by

Cheryl Driscoll CIA, CGAP, CCSA, CRMA, CFE
Chief Audit Executive

Date

EXECUTIVE SUMMARY

Conclusion

We conclude that the departmental governance structure and corporate policy provide overall an effective management control framework for Emergency Management and Business Continuity Planning in the Department of Justice. The structure includes the Executive Committee, the Emergency Response Committee, the Emergency Operations Team, the Justice Emergency Coordinating Committee, the Justice Emergency Team, the Justice Emergency Operations Centre and the National Security Business Continuity Planning Committee. The key corporate policies in place for these programs are the *Department of Justice Strategic Emergency Management Plan* and *A Guide to Business Continuity in the Department of Justice*.

Emergency Management and Business Continuity Planning are two distinct but linked programs in the Department, which come together in a practical way in the Justice Emergency Operations Center. The Emergency Management program is external and strategic, while the Business Continuity program is internal and one of the building blocks in the development of the *Department of Justice Strategic Emergency Management Plan*.

We did not find significant issues with respect to Emergency Management.

Introduction

The Emergency Management program and the Business Continuity Planning program are both managed by a small section within the Safety, Security and Emergency Management Division in the Administration Directorate of the Management Sector. These programs are separate but complementary in nature – Emergency Management planning builds on Business Continuity Planning.¹

The Emergency Management program is focused on how the Department relates to other federal government institutions, as well as provincial and municipal emergency organizations, in emergencies. Business Continuity Planning, by contrast, represents the Department's internal planning associated with the continued availability of critical services to Canadians in the event of an incident/emergency affecting the organization. Business Continuity Plans are often activated when Emergency Management exercises or real events take place.

An industry benchmark is that no more than 10%-15% of an organization's services should be classified as critical.² There is a natural tendency for managers to identify important services as critical services and to require recovery too quickly.

¹ *Emergency Management Planning Guide, 2010-2011*, page I, paragraph 4

² *Business Continuity Planning Program Technical Documentation*, Public Safety and Emergency Preparedness Canada, p.26

The Department of Justice has developed and implemented a strong and effective departmental governance structure for Emergency Management and Business Continuity Planning. The *Strategic Emergency Management Plan* is current, well-written and contains all of the more than 30 recommended “building blocks” of the *Public Safety Canada Emergency Management Planning Guide, 2010-2011*.

The governance framework supporting emergency preparedness is defined within the Department’s *Strategic Emergency Management Plan* and clearly identifies the roles and responsibilities of various levels of management involved in emergency response. The presence of senior management on the Emergency Management committees conveys the proper level of authority to support the decision making process essential to address emergency situations.

The Department ensures preparedness of senior management responsible for the implementation of the *Strategic Emergency Management Plan* by conducting yearly exercises at off-site locations to test the emergencies addressed in the *Plan*. Furthermore, the Department has signed a Memorandum of Understanding with the Supreme Court of Canada in Ottawa, Ontario and the Canada School of Public Service in Gatineau, Quebec, for the use of operational space to be used by the Emergency Response Committee to meet and direct the Emergency Plan. The locations of the alternate operational facilities ensure that the Committee will be able to access at least one location.

The Justice Emergency Operations Center integrates a robust emergency management capability into an existing infrastructure. This facility has been used to conduct simulated emergency management exercises (e.g., desk top exercises), to manage and respond to such events as ice storms, and participated in large scale horizontal emergency exercises such as the Vancouver Olympics and the G8/G20 Summits in Toronto.

The assignment of Business Continuity Planning responsibilities to the Regional Security Officers has proven to be a pragmatic decision. Emergency Management and Business Continuity Planning agenda items are frequently raised in the regular Departmental Security Officer conferences, which are attended by Regional Security Officers. Also, the Departmental Security Officer conducts visits to the Regions on a regular basis.

This audit was identified in the *2011-12 Risk-Based Audit Plan*. The overall objective of the audit was to provide assurance that the management control framework is effective for Emergency Management and Business Continuity Planning in the Department of Justice.

Key Findings

The section in the Safety, Security and Emergency Management Division responsible for the departmental Emergency Management and Business Continuity Planning programs is currently comprised of two full-time resources³ - one AS⁴ 07 Emergency Management Manager and one AS 05 Departmental Business Continuity Planning Coordinator. It is considered to be effective for its size. However, if additional resources were established in this small unit, the following additional priorities could be addressed, which constitute the major findings for this audit:

- **Challenge (Oversight and Quality Assurance) Function.** The Safety, Security and Emergency Management Division does not exercise an effective challenge (Oversight and Quality Assurance) function with respect to Business Continuity Planning across the Department. This has resulted in inconsistency of Business Continuity Plans, difficulty in the identification of critical services, and underuse/misapplication of documentation for Business Impact Analyses.
- **A Consolidated Corporate Business Continuity Plan.** A consolidated corporate Business Continuity Plan would help to ensure that critical services are identified at a practical level and save considerable effort currently expended on maintaining Business Continuity Plans for important, but not necessarily critical, services.
- **Support to the Regions.** The Regional Offices would benefit from additional support and mentoring from the Safety, Security and Emergency Management Division with respect to Business Continuity Planning. There is considerable risk associated with the current situation in conjunction with modernization initiatives.

³ In the *2007 Report on a Tabletop Exercise*, M. Purdy recommended a small centre of expertise on emergency management that should include at least three positions, ideally staffed by public servants with extensive relevant experience and credentials. We understand this to be separate from positions required for the Business Continuity Planning program.

⁴ AS refers to the Administrative Services Group

1.0 INTRODUCTION

1.1 Background

1.1.1 The Emergency Management (EM) program and the Business Continuity Planning (BCP) program are both managed by a small section within the Safety, Security and Emergency Management Division (SSEMD) in the Administration Directorate of the Management Sector in the Department of Justice Canada. This section is currently made up of one AS 07 EM Manager and one AS 05 Departmental BCP Coordinator. These programs are different but complementary in nature - EM planning builds on the BCP⁵.

1.1.2 The Department's Report on Plans and Priorities⁶ states that the annual budget for fiscal year 2012-13 is \$739.9M and the authorized Full-time Equivalents (FTEs), or personnel, are 5098. The corresponding information for SSEMD is a budget of \$1.148M and 16 FTEs.

1.1.3 The Emergency Management program is focused on how the Department relates to other federal government institutions, as well as provincial and municipal emergency organizations, in emergencies. It is external in focus and strategic in nature. BCPs, by contrast, represent the Department's planning associated with its "internal" efforts to ensure the continued availability of critical services to Canadians in the event of an incident/emergency affecting the organization. BCPs are often activated when EM exercises or real events take place.

1.1.4 The principal references or standards for EM and BCP are presented at *Appendix A*.

1.1.5 Two reports by M. Purdy in 2007⁷ and 2009⁸ set the agenda for the EM program in Justice Canada for several years. The recommendations in these reports were accepted as a baseline for EM by senior management and all but a few of the recommendations have been implemented.

1.1.6 *Emergency Management Program*. As illustrated at *Appendix B*⁹, the Department of Justice governance structure for EM is two-tiered, supported by three special-purpose teams. The first tier is the Emergency Response Committee (ERC) that provides strategic leadership and oversight for Emergency Management. The second tier is the Emergency Operations Team (EOT), the first responders that manage the ensuing emergency with support from legal counsel as required. The EOT is supported by the Justice Emergency Coordinating Committee (JECC),

⁵ *Emergency Management Planning Guide, 2010-2011*, page I, paragraph 4, Public Safety Canada

⁶ *Department of Justice Canada 2012-13 Report on Plans and Priorities, Section 1 Organizational Overview, Planning Summary, table titled Financial Resources, and table titled Human Resources (Full Time Equivalent – FTEs)*

⁷ *Report on Tabletop Exercise, Justice Canada, September 13, 2007*, M. Purdy

⁸ *Report on Tabletop Exercise, Justice Canada, October 8, 2009*, M. Purdy

⁹ Adapted from Figure 4, p.16, *Security Program Governance Structure*, Department of Justice *Departmental Security Plan 2012-2015*, dated December 2012

which coordinates the legal and corporate advice from both the EOT and the Justice Emergency Team (JET) through the Justice Emergency Operations Center¹⁰ (JEOC).

1.1.7 The *Department of Justice Strategic Emergency Management Plan (SEMP)* sets out an organized, structured approach to decision making to enable the Department to deal effectively with situations requiring extraordinary efforts. It is based on the *Emergency Management Planning Guide, 2010-2011*, published by Public Safety Canada.

1.1.8 Emergency management has been an active file in the Department since 2007. Recently, Public Safety Canada has published *SEMP Leading Practices*¹¹ and identified criteria used to rate federal government departments' SEMPS. Although outside the scope of this audit, it was observed that the Department has already instituted most of the leading practices recommended by Public Safety, and has a few additional leading practices to offer, in particular, the design and operation of the JEOC.

1.1.9 *BCP Program.* The Department has developed a department-wide Business Continuity Planning Program to ensure critical service delivery within the Department. *A Guide on Business Continuity Planning in the Department of Justice* has been developed to assist departmental organizations in developing business continuity plans and to outline a uniform approach to plan development. SSEMD recognizes that this *Guide* should be updated.

1.1.10 As illustrated at **Appendix B**, the departmental BCP Coordinator is part of the National Security Business Continuity Planning Committee (NSBCPC) that is chaired by the Departmental Security Officer (DSO), who is also a member of the ERC.

1.1.11 In addition to the *Policy on Government Security (PGS)* that provides general policy on BCP, the *TBS Operational Security Standard – Business Continuity Planning Program* provides more specific definitions and procedures.

1.1.12 An industry benchmark is that no more than 10%-15% of an organization's services should be classified as critical¹². There is a natural tendency for managers to identify too many critical services and to require recovery too quickly. In other words, managers tend to identify important services as critical.

1.1.13 Public Safety Canada has recently indicated that it will be moving forward with BCP renewal initiatives in the near future.

¹⁰ *Department of Justice Emergency Management Plan*, dated May 01, 2012, p.15

¹¹ *Public Safety Canada, Strategic Emergency Management Plans (SEMPs) Leading Practices 2010-2011*

¹² *Business Continuity Planning Program Technical Documentation, Public Safety and Emergency Preparedness Canada, p.26*

1.1.14 *JEOC*. The EM and BCP programs come together in a practical way in the JEOC. The JEOC has been used to conduct a high level of exercises and events for both EM and BCP. Between September 2007 and March 2013 more than¹³ 85.5 days of EM exercises/events were conducted. For the period September 2009 to September 2012, more than¹⁴ 33.5 days of BCP exercises/events were conducted. This activity is described¹⁵ at *Appendix C* and *Appendix D* for EM and BCP respectively.

1.1.15 Some of the main features of the JEOC are described at *Appendix E*.

1.1.16 *Audit Approval*. The audit of the Emergency Management Program and the Business Continuity Planning Program was included in the *2011-12 Risk Based Audit Plan*, as approved by the Deputy Minister.

1.2 Audit Objectives and Scope

1.2.1 The objective of this audit was to provide assurance that the management control framework in the Department of Justice is effective for Emergency Management and Business Continuity Planning.

1.2.2 The scope of the audit was strategic rather than technical in nature, as is reflected in the criteria selected for this audit and in the findings of this report. The audit covered all activities related to EM and BCP in headquarters (National Capital Region) and the Regions.

1.3 Risk Assessment

1.3.1 The key risk factors that were considered in relation to this audit include:

- Adequacy of resources across the Department to carry out EM and BCP program responsibilities, including the Regions;
- Capability to communicate with other federal government agencies during real events;
- The transition of the transfer of the bulk of departmental information technology (IT) infrastructure to Shared Services Canada (SSC); and
- Oversight and Quality Assurance (QA) of the BCP program.

1.4 Audit Criteria

1.4.1 Two high-level lines of enquiry – Governance and Risk Management - and related audit criteria (as presented at *Appendix F*) were selected to provide a strategic perspective of the EM and BCP programs. These were developed in consideration of the risks identified during the planning phase of the audit and were based on guidance from *the TBS Management*

¹³ Does not include time for internal briefings, conferences, Exercise design, conduct and lessons noted.

¹⁴ Ibid footnote 13

¹⁵ Provided by SSEMD.

Accountability Framework, the TBS Core Management Controls: A Guide for Internal Auditors, and the standards/references for EM and BCP presented at **Appendix A** .

1.5 Approach and Methodology

1.5.1 The audit was conducted during two different time periods. The audit work in 2011 concentrated on Business Continuity Planning, while the audit work in 2012-13 focused on Emergency Management.

1.5.2 A detailed description of the approach and methodology is outlined in **Appendix G** of this report.

1.6 Identified Strengths

1.6.1 The Department of Justice has developed and implemented a strong and effective departmental governance structure for EM and BCP. The *SEMP* is current, well-written and contains all of the more than 30 recommended “building blocks” of the *Public Safety Canada Emergency Management Planning Guide, 2010-2011*.

1.6.2 The governance framework supporting emergency preparedness is defined within the Department’s *SEMP* and clearly identifies the roles and responsibilities of various levels of management involved in emergency response. The presence of senior management on the EM committees conveys the proper level of authority to support the decision making process essential to address emergency situations.

1.6.3 The Department ensures preparedness of senior management responsible for the implementation of the *SEMP* by conducting yearly exercises at off-site locations to test the emergencies addressed in the Plan. Furthermore, the Department has signed a Memorandum of Understanding (MOU) with the Supreme Court of Canada in Ottawa, Ontario and the Canada School of Public Service in Gatineau, Quebec, for the use of operational space to be used by the ERC to meet and direct the Emergency Plan. The locations of the alternate operational facilities ensure that the Committee will be able to access at least one location.

1.6.4 The Justice Emergency Operations Center integrates a robust emergency management capability into an existing infrastructure. This facility has been used to conduct simulated emergency management exercises (e.g., desk top exercises), to manage and respond to such events as ice storms, and participated in large scale horizontal emergency exercises such as the Vancouver Olympics and the G8/G20 Summits in Toronto.

1.6.5 The assignment of BCP responsibilities to the Regional Security Officers (RSOs) has proven to be a pragmatic decision. EM and BCP agenda items are frequently raised in the regular Departmental Security Officer (DSO) conferences, which are attended by RSOs. Also, the DSO visits the Regions on a regular basis.

2.0 FINDINGS, RECOMMENDATIONS AND MANAGEMENT RESPONSES

2.1 Challenge (Oversight and QA) Function

Key Finding: SSEMD does not exercise an effective challenge (Oversight and Quality Assurance) function with respect to BCP across the Department. This has resulted in inconsistency of BCPs, difficulty in the identification of critical services, and underuse/ misapplication of documentation for Business Impact Analyses.

Audit Criterion 1: Appropriate governance structure and corporate policy are in place.

Audit Criterion 2: Risks are identified, assessed and mitigating strategies are in place.

2.1.1 *Inconsistency of BCPs.* We observed that the 17 BCPs for critical services in corporate headquarters¹⁶ varied in length from 14 to 73 pages, and on average were made up of 34% telephone contact lists. As illustrated at *Appendix H*,¹⁷ nine (of the 17) BCPs were outdated and eight were missing elements of the common format recommended in the *DOJ Guide to BCPs*. “Outdated” refers primarily to the annual updating of the telephone contact numbers in these BCPs.¹⁸ However, “outdated” can also refer to organizational and other changes that are not reflected in the BCP. For example, the Information Management Branch (IMB) BCP is outdated with respect to the Shared Services Canada initiative. Updating of the IMB BCP, in conjunction with the departmental BCP Coordinator, could provide a useful source document for all BCP coordinators in the Department.

2.1.2 The six BCPs we reviewed for the Regions varied from 21 pages to 250 pages in length, with an average of 36% being made up of telephone contact lists. Only one of the BCPs was outdated (with respect to telephone contacts) and two were missing elements from the common format in the *DOJ Guide to BCPs*, as illustrated at *Appendix I*. Modernization initiatives that are currently underway were not considered when reviewing the BCPs for the Regions.

2.1.3 Accordingly, consistency of BCPs could be improved in several ways. First, direction on the maximum length of BCPs could be provided in the *SEMP* to include the length of telephone recall lists, if they are included at all. Second, telephone recall lists, or large parts of them, could be moved to a separate document on an intranet website that could be updated regularly and cross-referenced in the BCP. Third, SSEMD could better monitor compliance with the common elements (template) in *the Guide to the BCP*, ensure the BCPs are current, and take follow-up action as necessary. Collectively, this is Oversight and QA.

¹⁶ *Department of Justice, Critical Services Information Collection*, prepared for Public Safety Canada, dated August 24, 2009.

¹⁷ Outdated and/or incomplete elements are annotated with an “X” at **Appendices H & I**.

¹⁸ The Departmental BCP Coordinator uses this information to update his “Quick Hit” lists for the JEOC.

2.1.4 *Identification of Critical Services.* Public Safety Canada recognized in a 2010 memo to Departments that “...there are differences in the interpretation of a critical service” We found this to be the situation in the Department. In our review of the 17 corporate BCPs identified to have critical services, we found that three did not have any critical services and that 11 identified critical services at the Program and Branch level rather than at the business line level. One exception, the 2013 BCP for the Family Orders and Agreements and Enforcement Assistance Program, identified four critical functions and two necessary functions. This level of detail permits the identification of critical assets and the development of appropriate continuity procedures. Another exception, the BCP for the Chief Financial Officer Branch (CFOB), included a one page summary that described the critical services in adequate detail. In the review of Regional BCPs, one Region included several critical assets in its statement of 15 critical services. In this case, the large number of critical services identified and the confusion with respect to critical assets, demonstrates that some expert assistance would be helpful. Sophisticated analysis is required to identify critical services and critical assets. Overall, definition and mentoring across the Department with regard to the identification of critical services is warranted.

2.1.5 *Business Impact Analysis.* Business Impact Analysis (BIA) is the basic building block for BCPs, in that BIAs identify the critical services and critical assets that are used in the BCPs. However, BIA is not a widely used tool in the Department. The current list¹⁹ of seven departmental critical services with 17 corresponding BCPs was based on a series of BIAs developed in conjunction with the Y2K²⁰ Crisis in 1999. We have been advised by SSEMD that there has not been a significant re-examination of the fundamental analysis (BIAs) for the critical services and critical assets in these BCPs since that time. Similarly, there has been no significant re-examination of the BIAs for Regional BCPs for a number of years. There is a need to redo these BIAs to confirm the critical services and critical assets in corporate and regional BCPs.

2.1.6 The BIA process in the Department requires client organizations to complete a BIA Questionnaire but they are not provided with additional guidance or assistance. There is no specific training provided for the BIA process within the Department. The BIA Questionnaire was provided by Public Safety Canada and was posted on the Intranet in 2009. This form is lengthy, is not user-friendly and by itself is not conducive to the identification of critical services, which we would expect to be in the range of 10%-15% of total business lines²¹. There is no suitable explanation on the intranet site about how to use and apply the form.

2.1.7 We would expect an efficient BIA process to include a way to quickly filter services and processes that are not likely to be critical before the Questionnaire or other detailed analytical form is utilized. We are aware that other government departments have developed their own BIA process. A refinement and tailoring of the BIA process for the Department is warranted.

¹⁹ *Department of Justice, Critical Services Information Collection*, prepared for Public Safety Canada, dated August 24, 2009

²⁰ Year 2000 software problem

²¹ *Technical Documentation, Business Continuity Planning Program*, Public Safety and Emergency Preparedness Canada (Archived, undated)

2.1.8 *Responsibility.* SSEMD recognizes the responsibility for managing the departmental BCP program. We were advised that the priority for the past four years has been to design and implement the departmental emergency management governance structure. Now that this structure has been put in place, SSEMD anticipates that they can address issues related to BCP that they have been aware of for some time, as well as some additional issues raised in this report.

2.1.9 *Resources.* In the *2007 Report on a Tabletop Exercise*, M. Purdy recommended a small centre of expertise on Emergency Management that should include at least three positions²². We understand this to be separate from positions required for the BCP program. For the past few years at least, there have been only two full-time people assigned to EM and BCP - the BCP Coordinator who also manages the JEOC, works part-time on EM and carries out the standby function; and the EM Manager who has other security responsibilities as well.

2.1.10 *Risk Assessment.* We consider the risk associated with this finding to be **Medium**. Without an effective challenge function, these issues will likely not be resolved, that is, BIAs will not be done properly, BCPs will not necessarily identify the correct critical services, and extra effort will be expended on BCPs for non-critical services across the Department. We realize this risk is mitigated to some extent by the efficacy of the governance structure for EM.

Recommendation

- 1. The Director, SSEMD develop an action plan to improve the challenge (Oversight and QA) function with respect to BCP, to include refinement and improvement of the BIA process for the Department. (Medium Risk)**

Management Response

The Director, SSEMD agrees with the recommendation and will undertake the following actions:

- Provide the Emergency Response Committee and the National Security/Business Continuity Planning Committee with a briefing on the Internal Audit recommendations and Management Action Plan in September 2013;
- Develop a generic Business Continuity Planning template for business units that would ensure an integrated approach and consistency of Business Continuity Plans by March 2014;
- Review and update the Business Impact Analysis to make it more user-friendly in the identification of critical services and assets for business units by March 2014;
- Update the Departmental Guide for Business Continuity Planning by March 2014;
- Conduct training in the National Capital Region and the Regions on the re-vitalized business continuity planning program during the period from April to September 2014;
- Conduct an annual review of Business Continuity Plans and provide assistance and quality assurance feedback to business units on Plans beginning in fiscal year 2014-15; and,
- Provide biannual updates to the Emergency Response Committee and National Security and Business Continuity Planning Committee on the status of the Management Action Plans beginning in fiscal year 2014-15

²² *Report on Tabletop Exercise, Justice Canada, September 13, 2007, page 15, M. Purdy*

2. The Director, SSEMD develop a medium and long term human resources action plan to appropriately staff the EM/BCP function in SSEMD. (Medium Risk)

Management Response

The Director, SSEMD agrees with the recommendation and will undertake the following actions:

- Since the completion of the audit engagement, one position has been staffed; and,
- Review the staffing requirements for the long term to ensure that SSEMD meets the needs of the Emergency Management and Business Continuity Programs by November 2014

2.2 Consolidation of Corporate BCPs

Key Finding: A consolidated corporate BCP would help to ensure that critical services are identified at a practical level and save effort currently expended on maintaining BCPs for important but not necessarily critical services.

Audit Criterion 1: Risks are identified, assessed and mitigating strategies are in place.

2.2.1 In the 2009 Report On A Tabletop Exercise M. Purdy observed that, “DoJ does not have a consolidated, department-wide business continuity plan, but the SSEM Division has plans to do so, as a complement to the departmental Emergency Management Plan.”

2.2.2 The department-wide Business Continuity Plan was not developed. For the seven critical services identified in the 2009 Critical Services Information Collection²³, 17 BCPs have been developed. There are a total of 36 BCPs for the Department. Consolidation of these BCPs would significantly reduce the work required to update and maintain the BCP program in the Department.

2.2.3 As mentioned previously, there has not been a thorough re-examination of the BIAs supporting these 17 BCPs since 1999.²⁴ The result is that BCPs have been prepared for every organization on the list rather than only for those where critical services were identified. This could be described as encompassing “important” services as well as “critical services”. The result is extra work to maintain all of these BCPs and no guarantee that the critical services are properly identified.

2.2.4 Preparation of a consolidated corporate BCP, and eventually a departmental BCP, would help to resolve this situation. Appropriate action would entail a sophisticated BIA analysis that would consider all of the business lines/services and the corresponding critical assets. This one BCP could theoretically replace the 17 BCPs for central organizations that currently exist. It is anticipated that during the process some of the organizations involved would recognize that they do not have any critical services, as has already been the case with three of these organizations.

²³ Department of Justice, Critical Services Information Collection, prepared for Public Safety Canada, dated August 24, 2009

²⁴ We are aware that CFOB did complete two BIAs in 2009 for Resource Management and Policies, Systems and Corporate Accounting, but this did not include all financial processes.

2.2.5 This would also help the departmental BCP Coordinator identify the organizations that need a “hot seat” for the “Hot Site” he intends to develop in the primary Alternate Site whereby laptops for organizations with critical services would be maintained in a ready status.

Recommendation

3. The Director, SSEMD prepare a consolidated corporate BCP. (Medium Risk)

Management Response

The Director, SSEMD agrees with the recommendation and will undertake the following actions:

- Conduct a table top exercise with Emergency Response Committee members including Regions to validate the consolidated corporate Business Continuity Plan before March 31, 2014
- Upon completion of critical services review, a Departmental consolidated Business Continuity Plan will be tabled to the Emergency Response Committee for approval before March 31, 2015

2.3 Support to the Regions

Key Finding: Regional Offices would benefit from additional support and mentoring from SSEMD with respect to BCP. In the context of changes in reporting relationships stemming from Modernization Strategy consolidation initiatives, there are potential risks that some employees in Regional Offices may be overlooked in emergency situations.

Audit Criterion 2: Risks are identified, assessed and mitigating strategies are in place.

2.3.1 BCP Coordination is done on a part-time basis in the Regions, mostly by the Regional Security Officers (RSOs) who spend relatively little time on this activity.²⁵ Their experience and training with respect to BCP and EM varies considerably. As noted previously, this has resulted in inconsistency of BCPs, a wide variation in the identification of critical services and underuse/misapplication of BIAs. This situation presents opportunities for increased training and mentoring.

2.3.2 SSEMD confirmed that EM/BCP staff do not visit the Regions on a regular basis, but agrees that such visits are critical to the success of the BCP program. However, SSEMD does hold bi-weekly teleconferences with the RSOs, who are invited to attend BCP exercises in Ottawa. In addition, RSOs attend workshops with the DSO in Ottawa or when the DSO visits the Regions. The NSBCPC includes membership from all Regions but has not met recently – October 12, 2011 was the most recent meeting.

²⁵ One RSO estimated that he and his staff spend about 5% of their time on BCP.

2.3.3 Nevertheless, as M. Purdy observed, there is a tendency “...to pay less attention to issues which may arise at a regional, as opposed to a headquarters level”.²⁶

2.3.4 Modernization Initiatives²⁷ have recently resulted in consolidation of most functional staff in the Regions; that is, they now report to the appropriate functional head in Ottawa rather than to the Regional Director General in the Region in which they are located. The related risk is that some staff may be overlooked in the reorganization from an EM/BCP perspective. For example, a consolidated group in a region might be included in the relevant corporate BCP but not be considered with respect to local emergency procedures for fire and building evacuation. SEMD has a role to ensure that this does not occur. We have also been advised that the overall reorganization with respect to security, to include EM and BCP, has not been entirely resolved at this point. The risk associated with this finding during the transition period is rated as **High**.

Recommendation

4. The Director, SSEMD develop an action plan to more fully project the BCP program to the Regions. (High Risk)

Management Response

The Director, SSEMD agrees with the recommendation and will undertake the following actions:

- An agenda item will be brought forward to the June 2013 meeting of the Emergency Response Committee to amend the current membership to include representation from all Regions beginning in fiscal year 2013-14;
- Increase contact with the Regions to provide awareness briefings and training to senior managers and Regional Business Continuity Planning Coordinators between February and June 2014;
- Involve the Regions in the development of standardized Business Continuity Planning processes and tools and exercises. SSEMD will provide oversight and quality assurance with respect to Emergency Management and Business Continuity Planning activities in the Regions on an ongoing basis beginning in fiscal year 2013-14; and,
- Involve Regions in table top exercises which will help build an understanding among Regional colleagues on Emergency Management and Business Continuity Planning issues on an ongoing basis beginning in fiscal year 2013-14.

²⁶ Report on Tabletop Exercise, October 8, 2009, page 15, M. Purdy

²⁷ Modernization Strategy – What’s New? January 2013 Update, from Barbara Ritzen, ADM Integration, email dated 2013 Feb 01

3.0 AUDIT OPINION/OVERALL CONCLUSION

3.1 We conclude that the departmental governance structure and corporate policy provide overall an effective management control framework for EM and BCP in the Department of Justice.

3.2 EM and BCP are two distinct but linked programs in the Department that come together in a practical way in the JEOC. The EM program is external and strategic, while the BCP program is internal and one of the building blocks in the development of the *SEMP*. EM is mainly limited to the departmental level and its inter-relationships with other government departments and agencies.

3.3 We did not find significant issues with respect to EM.

3.4 Regarding the BCP program, we found three significant issues – Challenge (Oversight and QA) Function, Consolidated Corporate BCP, and Support to the Regions - that merit senior management attention. These three issues are all connected by a fundamental resourcing issue. We do not think these problems would exist to the same extent if the BCP function was adequately staffed.

3.5 Less significant issues have been raised in a management letter.

APPENDIX A - STANDARDS/REFERENCES

Emergency Management

Emergency Management Act (2007), Statutes of Canada (2007)

Emergency Management Framework for Canada (2008), Public Safety Canada

Federal Emergency Response Plan (2009), Public Safety Canada

Federal Policy for Emergency Management (2009), Public Safety Canada

Emergency Management Planning Guide 2010-2011

Department of Justice Emergency Management Plan (latest revision 2013)

SEMPs Leading Practices, Public Safety Canada (June 2012)

SEMPs Rating Guide, Public Safety Canada (June 2012)

Business Continuity Planning

Policy on Government Security, July 1, 2009, Treasury Board of Canada Secretariat

Operational Security Standard – Business Continuity Planning (BCP), Treasury Board of Canada Secretariat

Departmental Security Plan (2013)

A Guide To Business Continuity Planning, Public Safety Canada,

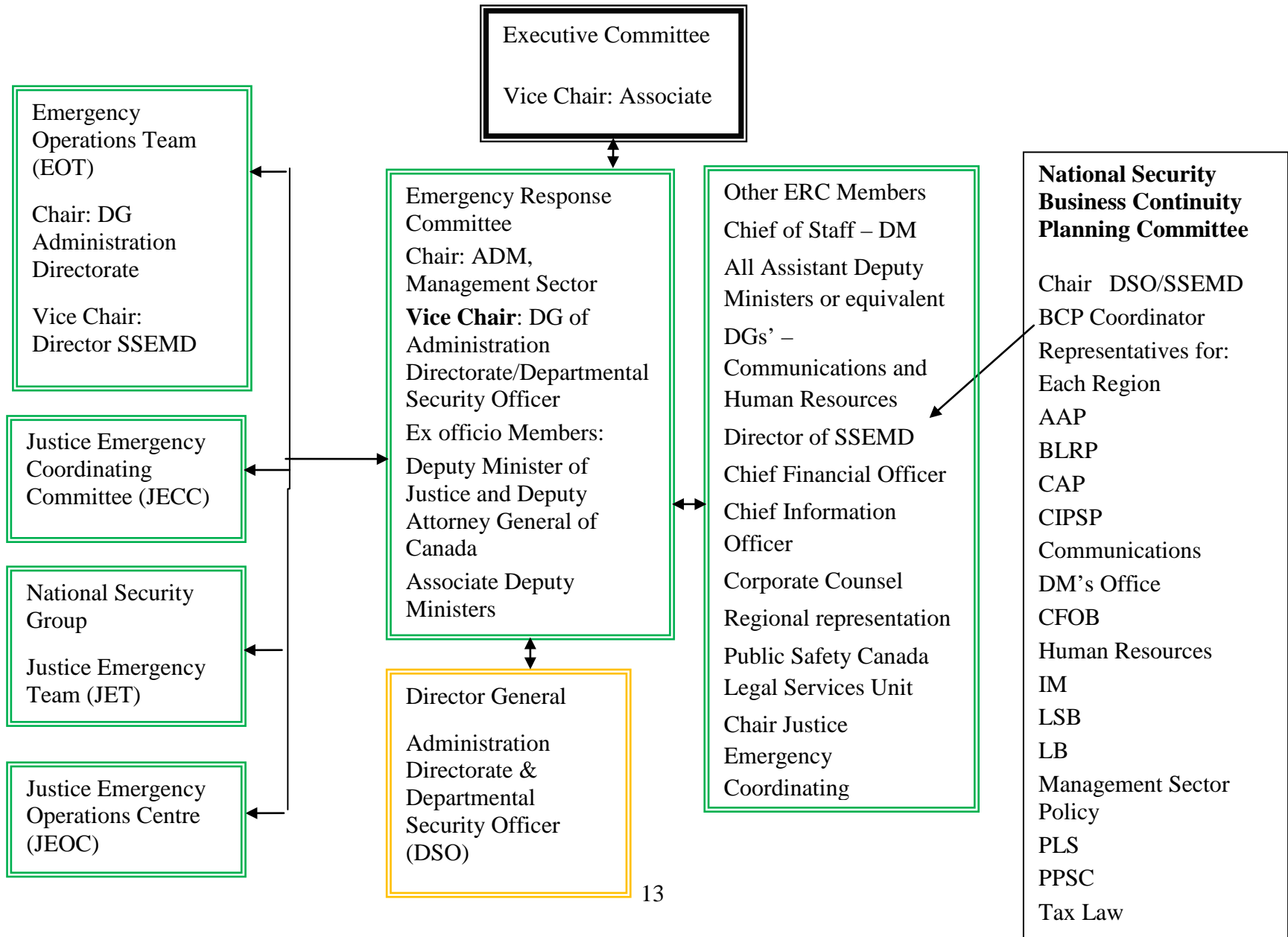
Directive on Departmental Security Management (2009), Treasury Board of Canada Secretariat

A Guide to Business Continuity Planning in the Department of Justice (latest 2011)

Justice BIA Questionnaire (2009)

Business Continuity Planning Program, Technical Documentation, Public Safety and Emergency Preparedness Canada (Archived)

APPENDIX B - EM AND BCP GOVERNANCE STRUCTURE



APPENDIX C – EM EXERCISES/EVENTS

Serial	Exercise/Event	Date	Days	Comment
1	Governing Council Exercise	September 13, 2007	1	Conducted by M. Purdy.
2	Exercise Governing Council	October 8, 2009	.5	Conducted by M. Purdy. Involved senior management
3	Exercise Silver, which included a Warm Start	February 2-5, 2009 February 9-13, 2009	10	
4	National Level Exercise	July 27-31, 2009	5	
5	Exercise Gold, which included a Warm Start	October 26 – November 1, 2009 November 2-6, 2009	11	
6	2010 Olympic and Paralympic Games	February 8-11, 2010 February 12-28, 2010 March 12-21, 2010	31	There was a preparation phase and then the actual events
7	Exercise Trillium Guardian, which included a Warm Start	May 3-8, 2010 May 10-14, 2010	11	
8	G8/G20 Summits	June 21-23, 2010 June 24-27, 2010	6	A preparation phase and then the event
9	Exercise Constant Guardian	January 26, 2011	1	
10	NATO Crisis Management, which included a Warm Start	October 17-18, 2011 October 19-24, 2011	7	
11	Exercise Due Vigilance	March 20-21, 2013	2	
	Total		85.5	

Notes:

1. The time information (days) in the chart does not include time for internal briefings, conferences, Exercise design, conduct, and lessons noted.
2. This information was provided by SSEMD.
3. EM events by definition usually involve senior management.
4. Warm Start - participants receive training and orientation prior to the actual event. This involves sending scenario injects (from the exercise controller) to the various players in the department requesting information and/or action.
5. NATO - North Atlantic Treaty Organization

APPENDIX D – BCP EXERCISES

Serial	Exercise/Event	Date	Days
1	Aboriginal Affairs Portfolio	September 2009	.5
2	Chief Financial Officer Branch	October 2009	.5
3	Public Law Sector	February 2010	.5
4	Northern Region	March 2010	.5
5	Policy Sector	May 2010	.5
6	Prairie Region	May 2010	.5
7	Tax Law	June 2010	.5
8	BC Region	October 2010	.5
9	Legislative Services Branch	November 2010	.5
10	Tax Law Sector	May 2011	.5
11	Emergency Response Committee	June 2011	.5
12	Aboriginal Affairs Portfolio	June 2011	.5
13	Communications Branch	September 2011	.5
14	Regional Security Officers	February 2012	.5
15	Central Registry of Divorce Proceedings	March 2012	.5
16	Family Orders and Agreements Enforcement Assistance Program	March 2012	.5
17	Ontario Region	September 2012	.5
18	BCP Warm Start for Exercises/Events throughout the period	Sep 2009 to Sep 2012	25
	Total		33.5

Notes:

1. The time information (days) in the chart does not include time for internal briefings, conferences, Exercise design, conduct, and lessons noted.
2. This information was provided by SSEMD.
3. Warm Start - participants receive training and orientation prior to the actual event. This involves sending scenario injects (from the exercise controller) to the various players in the department requesting information and/or action.
4. Both EM and BCP personnel are involved in the Warm Start training/orientation.

APPENDIX E - JUSTICE EMERGENCY OPERATIONS CENTER

The Justice Emergency Operations Centre (JEOC) is a facility which the Department can activate to support its integrated response to an emergency, an exercise or a disruption in service(s). The main function of the JEOC is to collect, collate and disseminate information during a disruption in service(s), an emergency situation, during a special event or, participation in government wide exercises.

Specifically, the JEOC:

- provides a 24/7 communications link to the Government Operations Centre managed by Public Safety Canada for operational information related to the emergency, and to other operations centres, including Regional Emergency Operations Centers, as required;
- alerts Department of Justice management and employees to an emergency situation and passes advice and communications messages to them, as authorized by the Emergency Response Committee;
- is the primary point of contact for sending/receiving documents and other communications relating to the emergency or exercise to/from the Department of Justice, Public Safety Canada, and external partners and clients;
- communicates information to decision makers through notification and situational reports and products prepared in accordance with the formats set out in the *Federal Emergency Response Plan* issued by Public Safety Canada; and,
- supports the Emergency Operations Team, the Justice Emergency Team and the Justice Emergency Coordinating Committee in their action planning efforts.²⁸

The JEOC located in the East Memorial Building consists of five rooms:

1. The Operations Room, which has several computers. This room can be run by one or two personnel. It has the capability to load images and videos onto screens in the other rooms in the JEOC. Other features of the Ops Room are:

- Satellite phones,
- DM's communications battle box: laptop, printer, BCP for Justice DM battle box and emergency contact lists, battle box; and
- DM's residence communication battle box with a small secure phone and satellite phone.
- Yellow box for BCP coordinator with larger satellite phone.

²⁸ Section 3.2.6, page 15, of the *Department of Justice Strategic Emergency Management Plan*, dated May 01, 2012

2. Primary meeting room – this has seating for about 15 people. It has screens that can be fed from the Operations room. This room is available for bookings for regular meetings.
3. Secondary meeting room – which is also available for normal bookings.
4. Boardroom - Large conference room for ERC and senior management. This seats up to 24, and includes high quality video service and the technology for simultaneous translation.
5. Private office – this room intended for a senior official in the event of a 24/7 event. It has office furniture, a communication facilities and a bed.

The JEOC also has the following facilities:

- Two bathrooms,
- Three locked cabinets,
- Plug and Go – technology which allows all 24 telephone lines in the other rooms to be moved to the main boardroom,
- a backup generator, and
- the capability to lock these operational areas down, by informing security at the front entrance of the building.

Alternate Sites

The primary alternate site for the JEOC is Canada School of Public Service (CSPS) in Gatineau, which is on a separate energy grid from that in Ottawa. As confirmed by an MOU, this facility can be used for a 24/7 operation. It is intended for longer term requirements.

A secondary alternate site has been arranged with the Supreme Court building, which is in close proximity to central Justice buildings. This site is much closer than the CSPS and is intended for emergency meetings of the ERC.

The CSPS facility consists of one large classroom about double the size of the Justice Boardroom. There is also an additional locked room, as well as a break-out room on request. Up to 23 laptops can be plugged in at one time using the CSPS network.

APPENDIX F – AUDIT CRITERIA

The following two high-level lines of enquiry – Governance and Risk Management - and related audit criteria were selected to provide an insightful perspective on the strategic elements of the EM and BCP programs. These were developed in consideration of the risks identified during the planning phase of the audit and were based on guidance from the *TBS Core Management Controls: A Guide for Internal Auditors*, and the standards/references for EM and BCP at **Appendix A**.

The results from our audit for each line of enquiry/criteria are presented for the EM and BCP programs respectively, in the right hand column of the chart below. Findings are presented in Section 2 of this report for those elements that are “Partially Met”.

Line of Enquiry	Criteria	Program	Results
Governance	1.0 Appropriate governance structure and corporate policy are in place	EM	Met
		BCP	Partially Met
Risk Management	2.0 Risks are identified, assessed and mitigating strategies are in place	EM	Met
		BCP	Partially Met

APPENDIX G – APPROACH AND METHODOLOGY

The audit was undertaken in a manner consistent with the *TB Policy on Internal Audit* and related guidelines and procedures, and with generally accepted auditing standards.

The methodology consisted of a review of corporate and regional documentation systems, practices, procedures and interviews with appropriate Department of Justice management and staff at headquarters and in two Regions.

In conducting this audit, the audit team:

- Developed detailed audit criteria for EM and BCP;
- Prepared a detailed audit program based on the criteria;
- Interviewed departmental management and staff;
- Conducted teleconference with one Region and an on-site visit to another Region.
- Conducted interviews with senior management in the JET and JECC;
- Further to the standards at Appendix A, reviewed the following documents:
 - *Public Safety Canada, SEMP Rating Guide,*
 - *Public Safety Canada, Leading Practices,*
 - *M. Purdy's Post-exercise Reports 2007 and 2009,*
 - *Terms of Reference for the Department of Justice National Security Business Continuity Planning Committee,*
 - *Departmental Security Plan,* dated January 2013, and
 - Departmental briefing decks on EM and BCP.
- Reviewed several audit reports of EM and BCP in Other Government Departments.
- Prepared a time-line for EM and BCP.
- Prepared a risk assessment for EM and BCP.
- Developed a SEMP/BCP Relationship Chart.
- Reviewed the *Collection of Critical Services* provided to Public Safety Canada in 2009.
- Reviewed 17 corporate BCPs and 6 Region BCPs for critical services compared to the common format recommended in the *A Guide to BCPs in DOJ.*
- Reviewed three corporate BIAs and ten BIAs for one Region.
- Compared *DOJ SEMP* to Public Safety Canada's SEMP template.

- Developed suggestions for strategic issues for consideration in an annual EM Work Plan.
- Developed suggestions for the *A Guide to BCP in DOJ*.
- Developed suggestions for the *Department of Justice SEMP*.
- Compared a new BCP template to common format of *DOJ A Guide to BCP in DOJ*.
- Developed an intelligence information flowchart.

APPENDIX H – CORPORATE BCPs – OUTDATED &/OR MISSING ELEMENTS

Serial	Element of Common Format	IMB	LB	PS	BRLP	CLB	PSDIMP	CRDP	PLS	TLS	Comm	DMO	SSEMD	MSADM
1	<i>Outdated? More than one calendar year has passed since last version published, or a significant organizational, technological or other development was not considered</i>	X		X		X	X	X	X	X	X	X		
2	Plan Overview - a description of the sector/branch, responsibility and primary role in the event of an emergency													
3	Plan Activation - the person responsible to approve the sector/branch's response in an emergency	X	X		X		X							
4	Governance Structure - defines the organization and identifies the executive team, project team, working group, the review and approval process and the communications and maintenance strategies.		X		X									
5	Threat Assessment and Impact Analysis - identifies and anticipates the impact of potential risks that may impact upon the sector/branch's ability to provide services to the rest of the Department.		X											X
6	Critical Services - those services or activities that must continue, albeit at a reduced level, in order for the Department to meet its mandate under adverse conditions (e.g. loss of access to a building)	X												
7	Site Response Team Members - list of personnel assigned to the response/recovery team.	X												
8	Physical Site Covered by the Plan - the departmental facility.			X			X							X
9	Disaster Assessment Procedures - the outline of procedures covered by the team manager and team members.													
10	Communications - how the manager/alternate, coordinator, team members and employees are contacted and the information being relayed.		X	X	X		X	X	X					X
11	Alternate Work Site - alternate work site and/or command centre.	X												X
12	Restoration of Operations and Services - the recovery strategy.	X	X	X	X				X					X
13	Continuity Requirements - the role and description of each team member during the recovery process.	X		X			X		X					X
14	Continuity Plan Training - an exercise designed to ensure that those employees who will be part of a Site Response Team are aware of their responsibility. The training can be a desktop exercise or depending upon time, financial and human resource constraints, more inter-active.	X	X	X					X				X	X
15	Assets and Interdependencies - assets include those facilities necessary to provide an acceptable level of service. The interdependencies include employees, clients, suppliers, external organizations and other government departments (federal, provincial and municipal).	X	X	X	X		X		X				X	X
16	Acceptable Delays - systems/applications that can only be unavailable for a limited period of time before it starts to have a negative impact upon the Department and the fulfillment of its mandate.	X	X	X	X		X		X				X	X

APPENDIX I – REGION BCPs – OUTDATED &/OR MISSING ELEMENTS

Serial	Element of Common Format	Atlantic	Quebec	Northern	Prairie	Ontario	BC
1	<i>Outdated. More than one calendar year has passed since last version published, or a significant organizational, technological or other development was not considered</i>		X				
2	Plan Overview - a description of the sector/branch, responsibility and primary role in the event of an emergency						
3	Plan Activation - the person responsible to approve the sector/branch's response in an emergency						
4	Governance Structure - defines the organization and identifies the executive team, project team, working group, the review and approval process and the communications and maintenance strategies.						
5	Threat Assessment and Impact Analysis - identifies and anticipates the impact of potential risks that may impact upon the sector/branch's ability to provide services to the rest of the Department.						
6	Critical Services - those services or activities that must continue, albeit at a reduced level, in order for the Department to meet its mandate under adverse conditions (e.g. loss of access to building, data, systems or workspace)						
7	Site Response Team Members - list of personnel assigned to the response/recovery team.						
8	Physical Site Covered by the Plan - the departmental facility.						X
9	Disaster Assessment Procedures - the outline of procedures covered by the team manager and team members.		X				
10	Communications - how the manager/alternate, coordinator, team members and employees are contacted and the information being relayed.						
11	Alternate Work Site - alternate work site and/or command centre.		X				
12	Restoration of Operations and Services - the recovery strategy.		X				
13	Continuity Requirements - the role and description of each team member during the recovery process.		X				X
14	Continuity Plan Training - an exercise designed to ensure that those employees who will be part of a Site Response Team are aware of their responsibility. The training can be a desktop exercise or depending upon time, financial and human resource constraints, more inter-active.						X
15	Assets and Interdependencies - assets include those facilities necessary to provide an acceptable level of service. These include employees, clients, suppliers, external organizations and other government departments (federal, provincial and municipal).		X				
16	Acceptable Delays - systems/applications that can only be unavailable for a limited period of time before it starts to have a negative impact upon the Department and the fulfillment of its mandate.						X

APPENDIX J – RISK ASSESSMENT GUIDELINES

Assessment*	Significance Level and Impact
High	<p>Immediate Management Attention Required</p> <p>IMPACT:</p> <p>Weaknesses exist that could impact the Department’s financial statements, reputation and/or the Department’s goals or objectives.</p> <p>Weaknesses could impact the Department’s efficiency and effectiveness of operations.</p> <p>Risk to the Department is significant.</p>
Medium	<p>Monitoring and Mitigation Required</p> <p>IMPACT:</p> <p>Weaknesses exist that could impact the entity’s financial records, the entity’s reputation, the entity’s goals or objectives or the efficiency and effectiveness of the entity’s operations.</p> <p>Risk to the Department is moderate.</p>
Low	<p>Improvement Required</p> <p>IMPACT:</p> <p>Opportunities are identified that could enhance operations by improving efficiency, effectiveness or control.</p> <p>Risk to the Department is low.</p>

* It should be noted that, in applying the above criteria to a recommendation, Internal Audit Branch takes into consideration the nature, scope, and significance of the audit finding(s), the impact of the recommendation on the organization, and the auditors’ professional judgment.

APPENDIX K – ACRONYMS/ABBREVIATIONS

AAP	Aboriginal Affairs Portfolio
AS 05 /AS 07	Refers to the Administrative Services Group.
BCP	Business Continuity Planning
BIA	Business Impact Analysis
BLRP	Business and Regulatory Law Portfolio
CAP	Central Agencies Portfolio
CFOB	Chief Financial Officer Branch
CIPSP	Citizenship, Immigration and Public Safety Portfolio
Comms Branch	Communications Branch
CSIS	Canadian Security Intelligence Service
CRDP	Central Registry of Divorce Proceedings
DM	Deputy Minister
DoJ	Department of Justice
DSO	Departmental Security Officer
DSP	Departmental Security Plan
EM	Emergency Management
EOC	Emergency Operations Team
ERC	Emergency Response Committee
FOAEA	Family Orders and Agreements Enforcement Assistance Program
FTEs	Full-time Equivalents – refers to the number of personnel
IIA	Institute of Internal Auditors

IMB	Information Management Branch
IT	Information Technology
JC	Justice Canada
JECC	Justice Emergency Coordinating Committee
JEOC	Justice Emergency Operations Centre
JET	Justice Emergency Team
LB	Litigation Branch
LSB	Legislative Services Branch
MAF	TBS Management Accountability Framework
NATO	North Atlantic Treaty Organization
NSBCPC	National Security Business Continuity Planning Committee
OGD	Other Government Department
PGS	Policy on Government Security
PLS	Public Law Sector
PPSC	Public Prosecutions Service of Canada
RSO	Regional Security Officer
SEMP	Strategic Emergency Management Plan
SSEMD	Safety, Security and Emergency Management Division
TB	Treasury Board
TBS	Treasury Board Secretariat
Y2K	Y2K is a common abbreviation for the year 2000 software problem

APPENDIX L – INTERVIEWS/MEETINGS BY POSITION

DG Administration

DG Information Management Information Management Branch

Director General Prairie Region

Senior Counsel and Assistant Director Legislative Law Services

Member of Justice Emergency Coordinating Committee

Chair of Justice Emergency Team

Director Safety, Security and Emergency Division

Director Family Law Assistance Services, Policy Sector

Director Business Management Tax Law Services

Director Library Services

Director Aboriginal Law Services Prairie Region

Director Information Management Edmonton

Special Adviser to the Director, SSEMD

Business Manager Chief Financial Officer Branch

IT Technical Team Lead, FOAEA and CRDP Applications

Manager Emergency Management, SSEMD

Business Manager Public Law Sector

BCP Coordinator Northern Region

Departmental Business Continuity Planning Coordinator

Information Management Branch BCP Coordinator

Shared Services Canada IT Infrastructure (Justice) Manager

National Security Group Security Analyst – Litigation Branch

Regional Security and Accommodation Officer Prairie Region