

TABLE OF CONTENTS

STATEMENT OF ASSURANCE	i
EXECUTIVE SUMMARY	1
1. INTRODUCTION.....	7
1.1 Background.....	7
1.2 Organizational Responsibilities.....	8
1.3 Audit Objectives and Scope	10
1.4 Audit Methodology.....	10
2. FINDINGS—MANAGEMENT FRAMEWORK	13
2.1 Mandate and Policies.....	13
2.2 Roles and Responsibilities.....	15
2.3 Risk Assessments and Business Continuity Plans.....	18
2.4 Management Reporting	20
2.5 Resources.....	21
2.6 Coordination and Linkages.....	22
3. FINDINGS—BUSINESS CONTINUITY PLANS	27
3.1 Training and Development	27
3.2 Content and Clarity.....	28
3.3 Evaluation and Testing	33
4. FINDINGS—BACKUP PROVISIONS	35
5. FINDINGS—POST-MORTEM REPORTS	37
6. FINDINGS—SECURITY IN EMERGENCY AND INCREASED THREAT SITUATIONS	39
7. FINDINGS—LEGAL SERVICES UNITS.....	41
8. FINDINGS—COMPLIANCE WITH GOVERNMENT POLICIES	43
9. RECOMMENDATIONS AND MANAGEMENT RESPONSE.....	45

STATEMENT OF ASSURANCE

We have completed the internal audit of business continuity planning. The overall objectives of the audit were:

- a) to review and assess the adequacy of the framework in place to support business continuity planning;
- b) to review and assess a sample of business continuity plans and to recommend improvements.

The internal audit was conducted in accordance with the Treasury Board Secretariat (TBS) *Policy on Internal Audit* and the Institute of Internal Auditors *Standards for the Professional Practice of Internal Auditing*.

- a) The audit team assessed the management control framework against criteria documented in TBS and departmental policies.
- b) The audit team assessed the management control framework against criteria derived from the requirements of the TBS, the *Emergency Preparedness Act*, the *Government Security Policy*, and the *Operational Security Standard - Business Continuity Planning (BCP) Program*.
- c) The audit team assessed the extent to which existing business continuity plans meet departmental requirements for the delivery of essential services during a disruption.
- d) The audit team assessed the extent to which operations and procedures are managed with due regard to economy, efficiency, and effectiveness.
- e) The audit team assessed the extent and appropriateness of monitoring activities to ensure the ongoing relevance of business continuity plans.

In our professional judgment, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the conclusions reached and contained in this report. The conclusions were based on a comparison of the situations as they existed at the time of the audit and against the audit criteria. It should be noted that the conclusions are only applicable for the areas examined.

LIST OF ACRONYMS

BCP	Business Continuity Planning
BCPs	Business Continuity Plans
BCPC	Business Continuity Planning Coordinator
BCPCs	Business Continuity Planning Coordinators
CIO	Chief Information Officer
DBCPC	Departmental Business Continuity Planning Coordinator
DM	Deputy Minister
EMC	Emergency Measures Committee
FOAEA	Family Orders and Agreements Enforcement Assistance
GSP	<i>Government Security Policy</i>
IM	Information Management
IMB	Information Management Branch
IT	Information Technology
LOPORS	Legal Opinions and Precedents On-line Retrieval System
LSUs	Legal Services Units
MITS	Operational Security Standard: Management of Information Technology Security
MOU	Memorandum of Understanding
PSEPC	Public Safety and Emergency Preparedness Canada
PWGSC	Public Works and Government Services Canada
ROs	Regional Offices
SMB	Senior Management Board
SMS	Salary Management System
SOTAD	Security Operations, Telecommunications and Accommodations Division
TBS	Treasury Board Secretariat
TRA	Threat and Risk Assessment

EXECUTIVE SUMMARY

Introduction

In accordance with the *Government Security Policy (GSP)*, the continued delivery of government services must be assured during a disruption. Business continuity planning is a proactive process to ensure that essential services or products are delivered. In June 2005, the Auditor General of Canada recommended that departments and agencies be required to develop Business Continuity Plans (BCPs) on a priority basis and to test these plans at least every two years.

The Department of Justice Business Continuity Planning Program was started in the year 1998/99 and initial plans were ready for Y2K. There are currently 29 BCPs in the Department: 18 for Headquarters and 11 for regional offices (ROs).

This audit covered all activities related to business continuity planning in headquarters, a sample of regional offices, and selected legal services units (LSUs).

Organizational Responsibilities. The Department has a three-tiered framework for managing emergencies including business continuity planning:

- The Senior Management Board (SMB) chaired by the Deputy Minister is responsible for decision making and oversight;
- The Emergency Measures Committee (EMC) is responsible for decision support, operational support and incident management;
- Regional and Headquarters Response Teams (site-level teams) prepare and manage their respective business continuity plans.¹

In addition, the Security Operations, Telecommunications and Accommodations Division (SOTAD) is responsible for coordinating the overall development and testing of BCPs in the Department as well as reviewing BCPs.

¹ From the Emergency Plan of the Department of Justice.

Management Framework

Mandate and Policies. Mandates and responsibilities are described in departmental plans, guidelines, and individual BCPs. However, the Department of Justice does not have a BCP policy as required by government-wide standards. A departmental BCP policy is needed to consolidate authorities for the approval and activation of BCPs, and describe key responsibilities and linkages with the Emergency Measures Program and the Security Manual.

Responsibilities for Business Continuity Planning are set out in *A Guide to Business Continuity Planning in the Department of Justice*, 2006. This guide is a good reference but more clarity and consistency with related documents is required. Furthermore, we found inconsistencies with respect to approval authorities for BCPs in *A Guide to Business Continuity Planning in the Department of Justice*, information provided by the Departmental BCP Coordinator, and individual BCPs. The Emergency Plan does not describe the approval authorities for BCPs, which should be clearly defined and documented. Also, the linkages between the Emergency Plan and related documents should be clarified.

Roles and Responsibilities. The responsibilities for activation and implementation of BCPs are set out in the *Emergency Plan*, *A Guide to Business Continuity Planning in the Department of Justice*, and BCPs. According to the Emergency Plan, the Emergency Measures Committee (EMC) plays a key role in coordinating Business Continuity Planning. However, the EMC has been inactive since June 2004 and its members need training on their role with respect to business continuity planning. The Emergency Measures Committee should be reactivated and regular meetings held.

Risk Assessments and Business Continuity Plans. A Business Impact Analysis was completed in the year 1998/99 but only for the four departmental Government Wide Mission Critical Systems. Threat and risk assessments were later prepared for the Department of Justice in 2000/01 but they did not address the preparation of BCPs. Appropriate threat and risk assessments would provide essential information for management in developing BCPs (i.e. which ones should have priority, what are realistic recovery times (faster recovery requirements are more expensive to meet), and which options provide the best return).

The Department has completed BCPs for most essential functions but some important ones are missing or are still being prepared. A plan is required that documents activities to be completed for the effective operation of the BCP program including a list of required BCPs, completion of pending BCPs, testing of all BCPs, and capability of BCPs to meet business continuity requirements.

Management Reporting. We were informed that management only receives verbal briefings. In our view, written reports would improve control and provide better records of the status and progress of the Program. The reports should be distributed to interested and authorized parties.

Resources. There is a part-time Departmental BCP Coordinator as well as 29 BCP coordinators who spend varying amounts of time preparing BCPs (from 1 to 20 days per year respectively). We noted that the quality of a BCP corresponds to the amount of time spent by the BCP Coordinator, and most BCP coordinators spend insufficient time on BCPs. BCP coordinators should spend the appropriate time on necessary activities to complete BCPs.

We found that some BCPs do not take into account the capability or the cost of recovering functions within the times specified within the BCP. Currently, it is unlikely that most recovery times specified in the BCPs can be met. Specified recovery times in BCPs should take into account departmental capacity to meet them, and recovery options and costs should be prepared and presented to management.

Coordination and Linkages. We found that there is a process in place for coordinating the preparation and updating of BCPs. BCPs are updated each year and a copy of each revised BCP is sent to the Departmental BCP Coordinator. Also, teleconferences are held with the regional offices. However, several regional and headquarters BCP coordinators told us that they would like to have more exchange of information among BCP coordinators as well as with the Departmental BCP Coordinator regarding their BCPs. Coordination of the activities of the BCP coordinators should be improved.

Business Continuity Plans

Training. The Departmental BCP Coordinator informed us that he provides training on how to develop and manage BCPs. However, not all current BCP coordinators have asked for or received training. Training should be provided to BCP coordinators who have not received training.

Content and Clarity of BCPs. The BCPs we reviewed contain much useful information but lack clarity and good organization to effectively deal with major disruptions. Despite this, a few BCP coordinators will be able to use their BCPs effectively because they have taken the time to become very familiar with them and have held discussions within their immediate area concerning measures that go beyond those documented in their BCPs.

We noted common issues with respect to several BCPs. This is because BCP coordinators are provided with a template for the preparation of BCPs that sets out a standard format and sample

text for BCPs. However, the template needs to be reorganized and rewritten to ensure that deficiencies are addressed. Furthermore, the terminology used in BCPs should be reviewed and clarified and their organization improved.

A few sectors/branches/regional offices have instituted additional procedures for business continuity that are not referred to in the BCPs. All important information should be included in BCPs.

We found the scope of the BCPs regarding the time period or activities they cover to be unclear. The Departmental BCP Coordinator informed us that BCPs need only address the immediate 30-day period following an interruption of services. Yet, the Emergency Plan states “Business Continuity Plans involve the resumption of operations, the repairing of property, and the re-establishment of services after the Department has been hit by a disaster.” BCPs indicate as their goal the same scope defined in the Emergency Plan. However, most BCPs address the continuity of essential operations for only short time periods and there is no plan to address continuity when the division/sector has not returned to normal operations within 30 days or longer. The scope of BCPs should be clearly and consistently defined in the Emergency Plan, *A Guide to Business Continuity Planning in the Department of Justice*, and the BCPs. Also, the transition to normal operations should be documented in the BCPs or, if documented separately, should be linked to the BCPs. Furthermore the BCPs should document any limitations, results of testing, any arrangements with suppliers or other organizations, backup facilities and required equipment.

Evaluation and Testing of BCPs. The Departmental BCP Coordinator reviews all BCPs for essential functions. However, there is little or no feedback to BCP coordinators on the results. In our review of a sample of BCPs, we found that improvements to the review process are required and that more feedback should be provided to the BCP coordinators. A review by a single individual is not sufficient; a review by a committee or a group established for such a purpose would be better.

BCPs are not complete until they have been tested, results of the testing documented, and revisions made as a result of the testing process. Various degrees of testing are possible. However, BCPs in the Department of Justice have not been tested.

Public Safety and Emergency Preparedness Canada (PSEPC) distributed a Quick Scan questionnaire in December 2005 to all government departments as part of an initial assessment of the BCP programs. The questionnaire consisted of 17 questions addressed to DMs. The questions required one of two responses: whether a requirement was met or not met. The questionnaire did not allow for answers with respect to partially met requirements. The Department answered that all requirements were met. However, based on our review of our sample of BCPs and the

information we obtained, 11 questions could have been answered as met between 50% and 100%, 4 as met by less than 50%, and 2 as practically not met. Because of the limited response options in the Quick Scan questionnaire, the results do not accurately reflect the status of BCPs in the Department.

Backup Provisions

Backup processes for IT data and software are generally appropriate. Usually, there is off-site backup of data and software each night. However, we were told that one regional office has weekly and not daily off-site backup. Furthermore, some backup sites are located within close proximity of the primary site. It is unclear to us whether copies of all required computer documentation, application source code, and original software media are kept off-site.

We found that off-site hardware backup to meet recovery requirements is insufficient and has not been tested to ensure essential services recovery in case of disaster. Also, plans to obtain the backup hardware when it is needed are not documented. For Headquarters, the Information Management Branch (IMB) has an agreement with Public Works and Government Services Canada to use a site. [Text Removed]

Recovery kits that are stored at alternate sites can facilitate recovery. These kits contain copies of essential records and references, the BCP (in paper and electronic removable media formats), necessary forms, and any other items that may facilitate business continuity. Some BCP coordinators have prepared or are in the course of preparing basic recovery kits. The recovery kit for one BCP Coordinator contained insufficient and obsolete material, and was stored at the primary site. Recovery kits should be prepared, referred to in BCPs, and stored at alternate sites.

Post-Mortem Reports

Post-mortem reports identify issues and ensure that needed improvements are made to BCPs. We found that post-mortem reports have been prepared but not for all situations in which BCPs were used or operations were interrupted.

Legal Services Units

Approximately 40 LSUs offer essential services to clients. We were told that in the event of a disaster or other interruption at their primary facilities, they must continue to provide some services within hours or at the most within one day. LSUs are supported by the client department and the Department of Justice. The Department of Justice takes the position that LSUs are covered by the BCPs of the client departments and there is no need for it to take further action. The Department has provided no guidance to LSUs with respect to business continuity. Furthermore, there are no BCPs for the services that the Department provides to LSUs. Yet the post-mortem report prepared by the Department after the August 2003 power failure in Ontario stated the need to include LSUs in the BCPs of the Department. Our interviews also indicated that some BCP coordinators understand the need to include LSUs in their BCPs. In our interviews LSUs indicated that they require BCP support from the Department. Most of the LSUs we interviewed have little knowledge of BCPs. The Department of Justice BCPs should address the continuity of services provided to LSUs and should provide training to LSUs with respect to business continuity planning.

Compliance with Government Policies

The Department of Justice has made progress but needs to improve compliance, as discussed throughout the report, with departmental policies and standards, the *Government Security Policy*, the *TBS Operational Security Standard - Business Continuity Planning (BCP) Program*, and the *Operational Security Standard: Management of Information Technology Security (MITS)*.

The management response to the recommendations contained in this report was provided by the A/ADM, Corporate Services.

1. INTRODUCTION

1.1 Background

Business continuity planning is a proactive process to ensure that essential services or products are delivered during a disruption. Essential services or products are those that must be delivered to ensure survival, avoid injury, and meet the legal or other obligations of an organization. Continuity Planning is important in every organization as each is at risk from potential disasters (e.g. power blackouts, building destruction, pandemics) that can disrupt operations.

In accordance with the *Government Security Policy* (GSP), the continued delivery of government services must be assured through baseline security measures, business continuity planning including information management (IM) and information technology (IT) continuity planning, and continuous risk management.

In the federal government, the Treasury Board Secretariat (TBS) has issued the GSP and the associated *Operational Security Standard - Business Continuity Planning (BCP) Program*. Public Safety and Emergency Preparedness Canada (PSEPC) advises federal departments on the preparation of business continuity plans (BCPs) and monitors their implementation. PSEPC is also developing a BCP audit guide that is intended to be used by government departments in auditing the Business Continuity Planning Program. It plans to conduct audits and assessments of departmental BCPs. Furthermore, in the *Operational Security Standard: Management of Information Technology Security (MITS)*, 2004, TBS also gives a high priority to the completion of business continuity plans.

In June 2005, the Auditor General of Canada recommended that departments and agencies be required to develop BCPs on a priority basis and to test these plans at least every two years.

The Department of Justice Business Continuity Planning Program was started in the year 1998/99 and initial plans were ready for Y2K. There are currently 29 BCPs in the Department: 18 for Headquarters and 11² for regional offices (ROs).

² Large ROs such as the Ontario and Atlantic regional offices have subdivided their BCPs into multiple BCPs. (See "Risk Assessments and Business Continuity Plans".)

1.2 Organizational Responsibilities

The responsibilities for activation and implementation of BCPs are set out in the Department of Justice Emergency Plan, October 20, 2005 and in *A Guide to Business Continuity Planning in the Department of Justice*.

The Emergency Plan was developed within the context of the *Emergencies Act*, the *Emergency Preparedness Act*, and the *Government Security Policy*. The Emergency Plan sets out how the Department is to respond to emergencies or significant disruptions that could have a detrimental impact on the continuity of its business and also describes how the Department would manage its participation in a national or provincial emergency. The Emergency Plan is broader in scope than the departmental BCPs. Departmental BCPs are prepared as part of the Department's Emergency Plan management process.

The Emergency Plan indicates the responsibilities with respect to business continuity planning. It states: "The Deputy Minister chairs the Senior Management Board and has overall responsibility for the Emergency Plan including business continuity planning." and "The Department has a three-tiered framework for managing emergencies including business continuity planning:

- Senior Management Board (SMB) (decision making and oversight);
- Emergency Measures Committee (EMC) (decision support, operational support and incident management);
- Regional and Headquarters Response Teams (site-level response teams) and sector and DLSUs (legal advice and support)."

A Guide to Business Continuity Planning in the Department of Justice, January 2006 also describes the various responsibilities for business continuity planning.

The Security Operations, Telecommunications and Accommodations Division (SOTAD) is responsible for:

- coordinating the overall development and testing of business continuity plans in the Department;
- reviewing sector/branch/regional office plans.

The Senior Management Board (SMB) is responsible for:

- considering and giving guidance/direction on legal and policy issues;

- approving the recovery and communications strategy;
- allocating extraordinary resources as necessary.

The Emergency Measures Committee (EMC) is responsible for:

- coordinating the response to emergencies that result in a significant disruption to essential services;
- managing the overall recovery/response strategy, including the departmental communications strategy as approved by the Senior Management Board;
- addressing the business resumption issues once the emergency response and disaster recovery strategies have been activated.

Sector/branch heads/regional directors are responsible for:

- conducting business continuity planning within their sector/branch/regional office;
- approving all plans within their sector/branch/regional office;
- appointing a sector/branch/regional office Business Continuity Planning Coordinator (BCPC).

Unit/group managers are responsible for:

- ensuring that a Business Continuity Plan is developed if essential functions have been identified;
- approving planning priorities within their organization;
- ensuring that their plan is maintained, coordinated, updated, and tested regularly.

Sector/branch/regional office BCP coordinators are responsible for:

- coordinating the completion of the Business Impact Analysis questionnaire, which requests information on the impact of the disruption on providing services or continuing operations;
- coordinating the development and approval of BCPs;
- conducting initial and continued testing (every two years) and maintaining the plan.

A Guide to Business Continuity Planning in the Department of Justice states that: “The Information Management Branch is responsible for ensuring that the Department has an IT business recovery strategy to address the impact of any computer system disruption, including contingency plans/strategies for each system.” However IMB informed us that the Information Management Branch is responsible for ensuring that the Department has an IT business recovery

strategy to allow for the recovery of departmental computer systems at an alternate facility. This recovery capability will be incremental with systems recovered as per the order identified in the BCP systems availability priority list. System owners and IMB are jointly responsible for the preparation of system start-up kits for priority systems only. IMB is also responsible for coordinating Information Management and Library business continuity matters.

1.3 Audit Objectives and Scope

The objectives of this audit were to review and assess:

- the adequacy of the management framework in place to support business continuity planning;
- the appropriateness of the business continuity planning process in the Department, including related departmental plans;
- the level and appropriateness of activities undertaken to support the BCP process;
- the appropriateness of training, advice, and guidance provided to regional offices, Legal Services Units (LSUs), and departmental sectors;
- the extent and appropriateness of monitoring activities to ensure the ongoing relevance of business continuity plans;
- the extent to which policies and procedures comply with the requirements of Treasury Board Secretariat, the *Emergency Preparedness Act*, the *Government Security Policy*, and the *Operational Security Standard - Business Continuity Planning (BCP) Program*.

The audit covered all activities related to business continuity planning in headquarters, a sample of regional offices, and selected LSUs. The fieldwork was concluded in December 2006.

It should be noted that the *Federal Accountability Act (FAA)*, which was to be tabled on April 11 2006, made provisions to establish an office of the Director of Public Prosecutions (DPP). The FAA is expected to be passed in the fall of 2006 and this legislation will have significant repercussions for the Department of Justice overall. The fieldwork for this audit was undertaken prior to the tabling of the FAA.

1.4 Audit Methodology

The methodology consisted of a review of pertinent documentation and procedures, interviews with relevant staff, and appropriate testing.

We conducted interviews with:

- the Director, Security Operations, Telecommunications and Accommodations Division (SOTAD);
- the Departmental Business Continuity Planning Coordinator (DBCPC);
- a sample of business continuity planning coordinators (BCPCs) in four regional offices and three LSUs;
- staff of the Information Management Branch (IMB);
- appropriate Department of Justice personnel;
- representatives from Treasury Board and PSEPC.

2. FINDINGS—MANAGEMENT FRAMEWORK

2.1 Mandate and Policies

The Treasury Board of Canada Secretariat *Operational Security Standard - Business Continuity Planning (BCP) Program* requires departments to develop policies and standards to govern their BCP programs. The Department of Justice does not have a BCP policy, although mandates and responsibilities are described in departmental plans, guidelines, and individual BCPs. In our view a departmental BCP policy is required to consolidate approval authorities and describe key responsibilities and linkages with the Emergency Measures Program and the Security Manual. The Security Manual currently does not refer to BCPs but we were told that it is being updated.

2.1.1 Approval Authorities

We found inconsistencies with respect to approval authorities for individual BCPs. The *Guide to Business Continuity Planning in the Department of Justice* states that the BCPs are to be approved by the head of the sector/branch/regional office and submitted to the Departmental BCP Coordinator for further approval. The Departmental BCP Coordinator informed us that BCPs are supposed to receive final approval from the Deputy Minister (DM) and that the DM did approve initial plans but has not continued to do so. The Emergency Plan does not describe the approval authorities for BCPs. Most individual BCPs indicate that they are approved by the head of the sector/ branch/regional office or by the DM. As a result, approval authorities vary from a director to the Deputy Minister.

We found that approval authorities for the activation of individual BCPs are also inconsistent and unclear. The Emergency Plan states that the Senior Management Board approves the activation of BCPs. In another section it also states: “The Emergency Measures Committee approves the activation of relevant corporate support service plans (Security Operations, Telecommunications and Accommodations Division (SOTAD), Information Management Branch (IMB) and site Business Continuity Plans).” Most BCPs indicate that their activation is approved by the local head/section/regional office. In our view, the requirement that a BCP’s activation should always be approved by the SMB is impractical and needs to be qualified. Disasters vary in nature and

extent. An immediate response may be required that cannot wait for authorization by a central committee. BCP coordinators told us that in the event of an emergency they would inform their immediate manager and take action right away. This is a good practical approach.

2.1.2 Key Responsibilities and Linkages

Responsibilities for business continuity planning are set out in *A Guide to Business Continuity Planning in the Department of Justice*, January 2006, which is available on the Security Web site of the departmental Intranet. This guide is a good reference but more clarity and consistency with related documents such as the Emergency Plan and the Security Manual is required.

We found issues with the linkages between BCPs and the Emergency Plan. In particular, there is no clear differentiation between emergency preparedness and business continuity planning. Also, neither the Emergency Plan nor any of the BCPs contain a glossary and there are no cross references. Furthermore, in the Emergency Plan there are references to both BCPs and Business Resumption Plans. It is unclear whether both terms are referring to the same type of plan or two distinct plans. The term “Business Resumption Plan” typically refers to a plan that focuses on resuming a business after essential operations have ceased, while the term “Business Continuity Plan” refers to a plan that endeavours to ensure that essential operations continue to be available during a period of disruption. However, sometimes the terms are used interchangeably to refer to one plan.

The Emergency Plan states, “The regional response to an emergency is set out in their individual Business Continuity Plans.” However, responding to an emergency does not fall within the purview of BCPs, since typically business continuity plans deal only with the continuity of essential operations after a major disruption has been experienced. Emergency plans have a much broader scope that addresses the response to an emergency.

The Emergency Measures Timeline (a separate document prepared by the Departmental BCP Coordinator) is a chart that attempts to summarize the sequence of actions to be taken and how staff are to be notified of emergencies. While such a document can be very useful, we note that the document does not include timeframes. Also, the chart needs revision (e.g. BCPs are included too late along the timeline to be effective) as well as an improved explanation on how to use it.

Recommendations and Management Response

1. It is recommended that the ADM, Corporate Services ensure that:

a) A departmental business continuity planning policy is developed.

Agree. A departmental BCP policy has been completed and is pending management approval.

b) The authorities for the approval and activation of BCPs are clearly defined and documented.

Agree. Once the authority process has been approved by the EMC it will be clearly defined and documented.

c) The *Guide to Business Continuity Planning in the Department of Justice* is made more clear and consistent.

Agree. The guide will be updated along with other related documents.

d) The linkages between the Emergency Plan and BCPs (and related documents) are clarified and that related documents use common terms and include cross-references, where appropriate.

Agree. A thorough review and comparison of these documents will be conducted so as to reflect any applicable linkages. This could include the creation of glossaries and electronic links as well

e) The scope of BCPs is clarified in appropriate documents to reflect that BCPs deal only with the continuity of essential operations.

Agree. The scope will be reviewed and clarified by the EMC and documented as appropriate.

2.2 Roles and Responsibilities

The responsibilities for activation and implementation of BCPs are set out in the *Emergency Plan* and *A Guide to Business Continuity Planning in the Department of Justice*. Various

responsibilities rest with the Deputy Minister, Senior Management Board, and the Emergency Measures Committee. SOTAD is responsible for coordinating the overall development, testing of business continuity plans in the Department, and reviewing sector/branch/regional office plans.

According to the Emergency Plan, the EMC currently has responsibilities for “decision support, operational support and incident management” with respect to business continuity planning. The Emergency Plan states: “The EMC is also responsible for addressing the Business Resumption issues once the emergency response and disaster recovery strategies have been activated and as more detailed assessment information becomes available.” It further states: “The Emergency Measures Committee will also manage the overall recovery/response strategy, which sets out the components of the recovery arrangements to be activated, including the departmental communications strategy as approved by the SMB.” Based on interviewees’ comments and the results of our review of a sample of BCPs, it is our opinion that BCPs require further review and that a committee³ or group should be established to supplement the review that is currently conducted by a single individual in SOTAD.

According to the Emergency Plan, the Emergency Measures Committee plays a key role in coordinating business continuity planning. However, the EMC has been inactive since June 2004 and its members need training on their role with respect to business continuity planning. Also, BCP coordinators do not clearly understand the role of the EMC for BCPs. We were told that one reason for the EMC’s inactivity is the frequent changes in its membership. We were also told that action is being taken to revitalize the Emergency Measures Committee (i.e. regular meetings). The Director, SOTAD and the Departmental BCP Coordinator are the key individuals who could advise the EMC and coordinate efforts in the Department.

BCPs in both Headquarters and regional offices are developed separately and, when activated, operate mostly independently of each other. However, in the event of a disruption, the activation of more than one BCP would be required to ensure the continuation of common essential services (e.g. IT, facilities, finance). Coordination between the various BCPs will therefore be important. In our view there is a need to clarify and document the role and responsibilities of key managers who provide common services to a Region or to the Department as a whole. In the event of a disruption these managers will be responsible for making appropriate decisions (e.g. regarding funding, communicating with the media). Clarification of their responsibilities with respect to business continuity planning would facilitate the role of the EMC.

³ We were told that a Business Continuity Planning Steering Committee existed in the past but was replaced by the Emergency Measures Committee (EMC). The role of the Business Continuity Planning Steering Committee was to oversee the implementation and maintenance of the BCP program, review and approve BCP policy, and review plans and make recommendations.

Furthermore, if a disruption affects multiple headquarters sites, coordination among BCP coordinators will also be extremely important and needs to be reflected in their responsibilities. Although the responsibilities of BCP Coordinators and the managers of the BCP program are outlined in various documents or guidelines, these responsibilities need to be consolidated and formalized in a policy. We found that BCP coordinators understand their roles and responsibilities and review their respective BCPs with managers in their sections. We also found that roles are generally well understood by most staff involved in BCP activities.

Recommendations and Management Response

2. It is recommended that the ADM Corporate Services ensure that:

- a) A committee or group is formed to review all BCPs and all substantive changes to BCPs.**

Agree. The formation of such a committee will be reviewed and discussed by the current Emergency Measures Committee and a decision will be made as to the structure of this new committee.

- b) The Emergency Measures Committee is reactivated and regular meetings are held.**

Agree. The EMC was reactivated and convened for a roles and responsibilities refresher as well as a tabletop exercise in June of 2006.

- c) Members of the EMC are trained in their role with respect to business continuity planning.**

Agree. BCP training was addressed in the form of “what if” scenarios and members were tasked with assisting in the rewrite of the Departmental Emergency Plan.

- d) The BCP responsibilities of key managers who provide common services to a region or to the Department as a whole are clarified.**

Agree. Key managers will be assembled to address this issue and documentation to clarify their position.

- e) The need for coordination among BCPCs is reflected in their responsibilities.**

Agree. Training sessions are being planned for all BCPCs for the Spring of 2007.

2.3 Risk Assessments and Business Continuity Plans

A Business Impact Analysis was completed in the year 1998/99 but only for the four departmental Government Wide Mission Critical Systems. Threat and risk assessments (TRAs) were later prepared for the Department of Justice in 2000/01 but they did not address the preparation of BCPs and are outdated. Also, no TRAs for business continuity planning have been prepared for the services provided to LSUs by the Department. The TBS *Operational Security Standard - Business Continuity Planning (BCP) Program* referred to in the departmental Emergency Plan requires that threat and risk assessments be completed to provide essential information for developing BCPs. Threat and risk assessments inform managers of the threats as well as the associated risks and resulting consequences of the threats, contain prioritized recommendations, and must be properly approved. TRAs allow management to determine to what extent it should invest in BCPs (i.e. which ones should have priority, what are realistic recovery times (faster recovery requirements are more expensive to meet), and which options provide the best return).

BCPs for most essential functions have been prepared but some important ones are missing. [Text Removed] Also, other functions would need BCPs such as the Legal Information Management Directorate, which supports iCase, an application system used by more than 4,000 staff members. Regarding the essential function of e-mail, interviewees at the Technology Services Division, IMB indicated they would likely test the e-mail recovery function at an alternate site in 2006, obtain specified recovery times, and assess whether these can be met. BCP coordinators for other BCPs also indicated they wished to test their BCPs. Furthermore, we were told that a pandemic preparedness plan is being considered that would impact on BCPs.

The large regional offices we reviewed have developed multiple BCPs. For example, the Ontario and Atlantic regional offices have approximately 12 plans each for their respective sections. These two regional offices have each created an umbrella plan to coordinate efforts in the event of the activation of multiple BCPs in their regions. Headquarters has developed 18 individual BCPs. Certain Headquarters services such as property management, accommodations, mail, and IT services are shared by sectors. However, Headquarters does not have an umbrella plan to assist in the efficient and effective coordination of the activation of multiple BCPs or establish overall priorities. In our view an umbrella plan for Headquarters is required.

The Emergency Plan refers to the need to evaluate the Departmental Consolidated Business Continuity Plan on a regular basis in accordance with the GSP. However, we found that there is no Departmental Consolidated Business Continuity Plan.

The Emergency Plan lists essential functions in general terms but the functions do not correspond to specific portfolios/units and there is no explanation of how they were selected. The list of IT services and application systems is incomplete. Also, the Emergency Plan does not include a list of key non-essential functions. For example, the National Accommodations and Occupational Health and Safety Division (NAOHS), which is responsible for obtaining new space for the Department, is an important function that is considered non-essential and therefore is not included. In our view, functions that provide support to essential functions such as the NAOHS should be designated as essential functions or key non-essential functions and identified in the Emergency Plan. We note that there is a BCP for NAOHS but it is not up-to-date.

The essential functions listed in the Emergency Plan do not correspond to the list of essential functions contained in BCPs. LSUs are referred to in the Emergency Plan but there is no reference to LSUs in the *Guide to Business Continuity Planning in the Department of Justice*.

We were informed by the Director, SOTAD, the Departmental BCP Coordinator, and the BCP coordinators that improvements to the BCP Program are planned. These include preparation of TRAs, revision of the Emergency Plan, testing of BCPs, improved alternate site backup for e-mail recovery by IMB, and completion of additional BCPs. However, there are no plans to complete pending BCPs (i.e. BCPs on which development efforts have begun or which have been identified as required).

Recommendations and Management Response

3. It is recommended that the ADM, Corporate Services ensure that:

- a) Threat and risk assessments are prepared that identify the business impact of not continuing certain functions and establish a complete and prioritized list of detailed functions, processes, and services that require continuity and recovery.**

Agree. TRAs will be conducted as required. A Security TRA at the national level is anticipated for FY 2007-08.

- b) A plan is documented and regularly updated that lists activities to be completed for the effective operation of the BCP program including a list of required BCPs, completion of pending BCPs, testing of all BCPs, and capability of BCPs to meet business continuity requirements.**

Agree. A document to accompany the current BCP Control Chart will be developed to further explain how the BCP Program runs and include all the benchmarks recommended.

c) An umbrella BCP is prepared for Headquarters.

Agree in principle. This will require discussion with PSEPC to determine parameters of this “umbrella” document given their lead role in government BCP preparation.

d) The preparation of a Departmental Consolidated Business Continuity Plan is considered, where beneficial.

Agree in principle. This will require discussion with PSEPC to determine need for “umbrella” plan and “consolidated plan”.

e) Services provided to LSUs by the Department are considered in the threat and risk assessments and are included in BCPs as appropriate.

Agree. Work is currently underway to establish MOUs between the Department of Justice and client departments for the provision of LSU services. BCPs will be addressed in these MOUs.

f) A plan is prepared for the completion of pending BCPs.

Agree. This will be completed by the departmental BCP coordinator in consultation with areas requiring plans.

2.4 Management Reporting

We were informed that management only receives verbal briefings. The Departmental BCP Coordinator provides regular briefings to the Director, SOTAD on the status of the Program. In turn, the Director, SOTAD briefs the Director General, Finance, Administration and Programs Directorate. We were also informed that briefings are provided to the DM when required and that the Senior Management Board would be briefed in April 2006.

In our view, written reports would improve control, provide better records of the status and progress of the Program, and could be distributed to members of the EMC as well as BCP coordinators who told us they would like to be better informed about the Program. The

management reports could cover planned actions, limitations of current BCPs, and risks associated with not having required BCPs.

Recommendations and Management Response

4. It is recommended that the ADM, Corporate Services ensure that written reports related to the BCP Program are prepared and distributed.

Agree. A written report will be provided to the ADMCS monthly.

2.5 Resources

The Departmental BCP Coordinator informed us that he spends about 80 percent of his time on BCP activities, that he has made significant progress with the BCP Program, and that his main expenses are for travel to regional offices.

There are 29 BCP coordinators who spend varying amounts of time preparing BCPs (from 1 to 20 days per year respectively). We noted that the quality of a BCP corresponds to the amount of time spent by the BCP Coordinator. Most BCPCs spend insufficient time on BCPs. As we discuss later in the report, we found that overall BCPs need improvement and that BCPCs should spend more time working on the BCPs. In addition to the BCP coordinators, other staff are also involved in work relating to the BCPs (e.g. updating contact lists and preparing sections of BCPs), and local managers assist in reviewing draft BCPs and suggesting changes. All BCPs identify a backup person for the related BCP Coordinator. However, for most of the BCPs we reviewed, the backup person has not been trained.

We found that some BCPs do not take into account the capability or the cost of recovering functions within the times specified within the BCP. No formal analysis of recovery options and costs has been prepared and presented to management to support informed decision making and requests for any additional resources. As we discuss later, it is unlikely that IT services can entirely meet the recovery times set in the BCPs. Nonetheless, regional IM/IT divisions and IMB at headquarters have taken steps to facilitate limited recovery. IMB has incurred expenses to rent an alternate site [Text Removed] and to acquire computer hardware, which will need to be maintained and replaced over time.

Recommendations and Management Response

5. It is recommended that the ADM, Corporate Services request that:

- a) **BCP coordinators spend the appropriate time on necessary activities to complete BCPs.**

Agree. Timing, implementation and control will be discussed and decided by the EMC.

- b) **A trained backup staff member is assigned for each BCPC.**

Agree. We strongly recommend the requirement for a trained backup BCPC for each plan although most already have one and are documented as such in their plans. This recommendation will be addressed in an annual BCP update reminder from the office of the ADMCS and will request a list of backups which will be trained by their respective BCPCs and SOTAD.

6. **It is recommended that the ADM, Corporate Services ensure that the specified recovery times take into account departmental capacity to meet them and that recovery options and costs are prepared and presented to management.**

Agree. Will require discussion with PSEPC to determine current framework for this information to be expressed to management.

2.6 Coordination and Linkages

We found that there is a process in place for coordinating the preparation and updating of BCPs. A list of 29 BCPs is maintained by the Departmental BCP Coordinator who is responsible for ensuring that the BCPs are updated each year and a copy of each revised BCP is sent to him. Furthermore, we were told that the list of contacts for each BCP is usually updated more frequently by the BCP coordinators.

Several regional BCP coordinators told us that they would like to have more exchange of information among BCPCs as well as with the Departmental BCP Coordinator regarding their BCPs. The DBCPC informed us that he conducts teleconferences with regional offices twice a year. We reviewed the agenda and the participation list of the last one held in January 2006. No minutes of the teleconferences were prepared. BCPCs at headquarters told us that the DBCPC has not conducted any group meetings with them. Also, several BCPCs (from both ROs and headquarters) told us that there are no conferences or meetings with other BCPCs; that they do not receive any feedback on their annual BCPs after these are sent to Headquarters; that they

have asked for but have not received copies of the Emergency Plan; and that they are not provided with information on the departmental BCP Program.

As stated above, BCP coordinators told us that they do not have a copy of the Emergency Plan. However, the Emergency Plan and BCPs are closely interlinked and Section 1.4 of the Emergency Plan states that the plan is aimed at “Business Continuity Plan Coordinators / Site Response Team Leaders.” Furthermore, the Departmental BCP Coordinator was not sure whether there are emergency plans for the regional offices and LSUs, or whether there are regional emergency coordinators who coordinate emergency measures with BCPCs. One region had a copy of an Emergency Response Life Safety Plan for its building that was prepared by PWGSC. Its Business Continuity Plan had no references to the building emergency plan, although they are related. The links between the Department’s Emergency Plan, building emergency plans, and the BCPs need to be clearly established in the various plans.

At Headquarters, staff in sections that provide common services to the Department (HQ and/or the regions) such as IT, finance, and facilities are not familiar with BCPs other than their own and do not know how their section would be affected if other BCPs are activated. This could delay responses if there are serious disruptions. We found that the BCPs in regional offices are reviewed by all those affected but this is not the case at headquarters. Therefore, there is a significant risk of inconsistency of recovery activities, plans, and schedules between the various BCPs in headquarters. In particular IMB’s directors need to review the BCPs of the sectors/branches/ROs that they service and agree to meet the recovery requirements of the BCPs. IMB representatives told us that they want to be involved in reviewing all BCPs.

We found that hardware and software requirements are not consistently listed in all BCPs. In some BCPs at Headquarters, hardware and software requirements are identified that fall within the responsibility of IMB. IMB representatives prefer that hardware and software requirements be identified in System Start-up Kits which are used to rebuild systems at the alternate computing facilities. A list of the hardware and software requirements should be included in BCPs or in System Start-up Kits. If not included in the BCPs, the BCPs should identify where the lists can be found.

The issue of sharing IT capacity across different sites has not been formally addressed. In the event of a disruption, hardware from another site can be used to provide backup to the disrupted site either by physically transporting the hardware or by transmitting data over communication links. Coordination of BCPs (both at HQ and in regional offices) is required for sharing backup equipment and facilities.

There is a BCP for the National Accommodations and Occupational Health and Safety Division (NAOHS), a key common services division, but we found that the BCP was not included on the DBCPC's list of BCPs. We also found that no alternate work site for the NAOHS was specified in the BCP. The NAOHS does not have any information on the BCPs of other sections. However, if a work site is down in the Department, the NAOHS is informed. It has a list of the space requirements for each section and is normally responsible (on a national basis) for approving space. The NAOHS does not have a list of alternate work site spaces or information on how soon the alternate work site space is required in order to resume normal operations.

The NAOHS also has responsibility for building services. We were told that the NAOHS would like to review all existing BCPs, and in our view, this division has the best capability to assess whether proposed alternate space in a BCP would meet the needs of the disrupted site. The NAOHS is the departmental authority for negotiating with PWGSC to obtain permanent space or undertake major renovations. It is unclear who has responsibility for coordinating the space allocated for the recovery of operations in the event of a disruption. The BCP coordinators, the Departmental BCP Coordinator, and the NAOHS would all need to be involved in this process. We were told that the NAOHS is not well prepared for the recovery of operations, which relates to our recommendation in "Risk Assessments and Business Continuity Plans" regarding the need for an umbrella plan for Headquarters.

Neither the Departmental BCP Coordinator nor the Manager, Security Operations, Telecommunications and Accommodations Division were aware of the BCPs for the Property Manager, the contracted property management company for two headquarters sites—the East Memorial Building and St. Andrew's Tower. [Text Removed] The Property Manager [Text Removed] informed us that the company is responsible only for regular routine building maintenance at the primary site (i.e. active site of operations). Should major work be required, PWGSC in consultation with the Department would need to proceed by means of a formal project. The Department requires increased coordination with PWGSC in the National Capital Region. Also, two of the three regional offices we contacted had held discussions with PWGSC regarding BCPs but had received no commitments in writing. The DBCPC needs to review the BCPs of contracted property managers and examine the issue of coordination with PWGSC. If the current situation is unsatisfactory, improved arrangements should be initiated.

Recommendations and Management Response

7. It is recommended that the ADM, Corporate Services ensure that:

a) Coordination of the activities of the BCPCs is improved.

Agree. This will happen throughout 2007-08 as the BCP Program plans are updated.

b) The departmental Emergency Plan is distributed to BCPCs.

Agree. To be distributed once it has been updated and finalized.

c) BCPs include clear linkages to building emergency plans.

Agree. The scope of all BCPs will be reviewed to ensure appropriate linkages are in place once the Departmental Emergency Plan has been reviewed, updated and approved by the Emergency Measures Committee.

d) Coordination among those Headquarters managers who play a key role in business continuity and recovery of normal operations is improved.

Agree. To improve coordination, common issues will be identified by the departmental BCP Coordinator who will meet with the managers as appropriate.

e) A list of hardware and software requirements should be listed in BCPs or in System Start-up Kits.

Agree. IMB plans to have this addressed in recovery kits for critical systems during FY 07/08. In order to minimize data maintenance problems and errors, this list will only be included in application specific recovery kits.

f) BCPs document the established arrangements with key suppliers and government departments that provide services in support of business continuity for the Department.

Agree. BCPCs will be advised to document this information as their plans are updated.

3. FINDINGS—BUSINESS CONTINUITY PLANS

3.1 Training and Development

The DBCPC informed us that he provides training on how to develop and manage BCPs. He provided BCP training at a regional security conference in Ottawa in February 2002. He also visited the Toronto regional office and delivered training to staff, and provided training to a few individuals from the Montreal regional office while they were in Ottawa. The Departmental BCP Coordinator informed us that he provides ongoing advice (e.g. on new developments or governmental decisions regarding BCPs) to regional BCPCs on request, but this advice is not often sought. Of the three regional BCPCs we contacted, one had received training. A second one had a brief discussion of the Region's BCP with the DBCPC but had not received any training, and the third one had not received training. The DBCPC has also offered to review BCPs individually with BCPCs at headquarters, but only one BCPC at headquarters had requested a consultation. The seven BCP coordinators we contacted at headquarters said that they had not received training. Staff from the Communications Branch told us that they had attended training given by the Privy Council and PSEPC related to communications in response to emergencies.

The Security Web site on the departmental Intranet contains BCP reference documents including *A Guide to Business Continuity Planning in the Department of Justice*. However, this is not used by the BCP coordinators we interviewed. As noted earlier in this report, this guide requires improvement and Headquarters needs to promote its use.

Recommendations and Management Response

8. It is recommended that the ADM, Corporate Services ensure that:

a) A list is maintained to indicate which BCPCs have received training.

Agree. The departmental BCP Coordinator will develop and maintain this list. The annual update memo will address training requirements.

b) Training is provided to BCPCs who have not received training.

Agree. To the extent possible as we need to be regularly informed of staff changes. Annual memo will address training requirements.

c) BCPCs are encouraged to refer to the information contained on the Security Web site that relates to business continuity planning.

Agree. A note to reflect this will be added to regular BCP update memos.

3.2 Content and Clarity

The BCPs we reviewed contain much useful information but lack clarity and good organization to effectively deal with major disruptions. Most BCPs we reviewed are problematic: terms used are not defined; there is no glossary; staff titles are incomplete; information is repetitive and inconsistent; and some sections contain information that does not relate to the section title.

Despite this, a few BCP coordinators will be able to use their BCPs effectively because they have taken the time to become very familiar with them and have held discussions within their immediate area concerning measures that go beyond those documented in their BCPs.

3.2.1 Deficiencies in BCPs

We noted common issues with respect to several BCPs. This is because BCP coordinators are provided with a template for the preparation of BCPs that sets out a standard format and sample text for BCPs. However, the template needs to be reorganized and rewritten to ensure that deficiencies are addressed.

Some missing or incomplete information we found in BCPs includes:

- The BCPs have varying lists of threats. While threats may vary across BCPs for valid reasons, important common threats are not always listed in all BCPs.
- The BCPs have inadequate provisions for ensuring the availability of backup personnel if the required staff are unavailable at the time of a disaster.
- There are no business impact assessments or some sections entitled Business Impact Assessment do not really explain the impact or the consequences to the business services of the Department.

- Recovery times and procedures are covered but some inconsistencies remain. In our opinion, a consolidated list or chart of recovery stages with target times and priorities, number of staff required, and key resources that the staff need should be included.
- There is no mention of disasters or interruptions that affect only part of a site.
- There is no mention of project management tools to be used during the business continuity process.
- There are no descriptions of considered recovery options and related costs either in the BCPs or any other document.
- The BCPs contain a list of required resources such as IT systems, but most do not have a complete list of other required resources (e.g. telephone, fax, courier services).
- The list of priorities for the recovery of IT services and application systems is incomplete since no mention is made of the IT infrastructure, which would need to be recovered prior to the recovery of any IT services and application systems.
- Most BCPs specify an alternate site but only for the response team and not for staff and other resources that would be required to continue services.
- Most BCPs do not contain complete inventories of required assets nor do they refer to where the inventory records are kept.

3.2.2 Recovery Times

Most BCPs contain inconsistent and unsubstantiated recovery times. As discussed in “Resources”, recovery times do not take into account the capability or the cost of recovering functions within the times specified in the BCPs. The recovery time for IT services is often set at eight hours, which in our view is too short a time period. BCPs should provide enough time to recover IT services. Also, there is often significant reliance on the quick recovery of central IT services to the exclusion of other measures (e.g. using telephones, faxes, information on CDs, or manual records). Yet these measures would allow for operations to continue until central IT services could be recovered. Some BCPs contain an assumption that is misleading. They cite the fact that BCPs will need to be activated if the “facility is not available (for any reason) for at least 30 days.” However, BCPs will need to be activated sooner than 30 days and this is stated elsewhere in the same BCPs. The BCP of one regional office has reasonable recovery times of 2 to 5 days for critical application systems, 20 days for essential functions, and over 20 days to restore remaining functions. Other BCPs specify recovery times as early as one day or eight hours for IT services. In our view these times are not reasonable or achievable with current resources. Recovery times need to be realistic and take into consideration costs and all required services for the function to continue, not just IT. Often, different parts of BCPs specify different recovery times for the same function. Also we found that BCP coordinators provided lengthier

recovery times once the implications of setting inadequate recovery times were explained during the audit process. Appropriate feedback to BCP coordinators is required.

As we mention later in this report, the BCPs we reviewed specify recovery times for some sectors/branches/ROs that in our view cannot be currently met. The BCPs also suggest that the process outlined in the BCPs is appropriate for the sectors/branches/ROs to recover. We found this is not accurate at this time for most of the BCPs we reviewed.

3.2.3 Scope

We found the scope of the BCPs to be unclear. The Departmental BCP Coordinator informed us that BCPs need only address the immediate 30-day period following an interruption of services. Yet, the Emergency Plan states “Business Continuity Plans involve the resumption of operations, the repairing of property, and the re-establishment of services after the Department has been hit by a disaster.” In our opinion, the scope as defined in the Emergency Plan that includes in the BCPs a transition to normal operations is more appropriate. BCPs indicate as their goal the same scope defined in the Emergency Plan. However, most BCPs address the continuity of essential operations for only short time periods and there is no separate process to address continuity when the division/sector has not returned to normal operations within 30 days. The time period covered by the BCPs should be extended or a separate process should be developed to link the BCPs to the recovery of normal operations. This could be addressed in the BCPs or in separate documents. In our opinion, it would be easier to link to the rest of the emergency and BCP process if the transition to normal operations were documented in the BCPs.

3.2.4 Additional Procedures

A few sectors/branches/regional offices have instituted additional procedures for business continuity that are not referred to in the BCPs. For example, IMB has developed procedures for the transfer of operations to its alternate site. These procedures are contained in a separate document. Since a major disaster or interruption will cause confusion and not all staff may be available when needed, it is important that the BCPs include complete documentation of the requirements, procedures, and arrangements needed to continue operations.

We found that the alternate sites specified in BCPs are often the homes of managers. If these locations are going to be designated as alternate sites, the BCPs need to contain information on required security, liability and expenses coverage, and whether proper services are in place (e.g. phones, faxes, and Internet connections).

On December 2005, Treasury Board Secretariat (TBS) issued to departmental directors of Human Resources a document on “Business Continuity with respect to Human Resources Matters.” The document provides advice to managers on:

- alternative working arrangements;
- provision of pay for employees who are unable to report to work due to office closures;
- leave for employees during an office closure;
- leave for employees directly affected by an emergency situation and/or those involved in providing emergency related services;
- temporary help agency personnel and/or contractors who are unable to work on federal contracts as a result of office closures.

This document contains information useful to those managing continuity of operations but it is not contained, summarized, or referred to in the BCPs.

Recommendations and Management Response

9. It is recommended that the ADM, Corporate Services ensure that:

- a) The terminology used in BCPs is reviewed and clarified and their organization is improved.**

Agree. A thorough review and comparison of these documents will be conducted by the departmental BCP Coordinator so as to clarify their organization and the terminology used.

- b) The template used for preparing BCPs is revised.**

Agree. Discrepancies or variances from standard or approved templates will be reviewed and our templates will be revised as necessary.

- c) All important information is included in BCPs.**

Agree. PSEPC will be consulted to determine what requirement Justice BCPs are missing.

d) Recovery times specified in BCPs are consistent within each BCP and substantiated.

Agree. BCPCs will be advised to substantiate recovery times as they update their plans.

e) The scope of BCPs regarding the time period or activities they cover is clearly and consistently defined in the Emergency Plan, the *Guide to Business Continuity Planning in the Department of Justice*, and the BCPs.

Agree. The scope will be clearly defined in all BCPs and associated plans and guides.

f) The transition to normal operations is documented and linked to BCPs.

Agree. Will require discussion with PSEPC.

g) The following are documented in BCPs: any limitations, results of testing, arrangements with suppliers or other organizations, backup facilities and required equipment.

Agree. The departmental BCP Coordinator will ensure that this information is documented in all BCPs as they are updated.

h) The departmental requirements and conditions including security considerations for the use of private homes with respect to business continuity planning are documented.

Agree. Will require discussions with PSEPC to verify requirements.

i) Any additional procedures for business continuity that are currently not part of the BCPs are included or referred to in the BCPs.

Agree. CBCPs will be reminded to include such documentation as part of the annual BCP reminder memo.

j) The document on “Business Continuity with respect to Human Resources Matters” issued by TBS is included, summarized, or referred to in the BCPs.

Agree. CBCPs will be advised of this document as they are reminded of their annual updates. The document will also be referred to in the annual BCP update memo.

3.3 Evaluation and Testing

As part of the development of new BCPs and during the yearly update of existing ones, the BCPs are submitted to the Departmental BCP Coordinator for review. However, there is little or no feedback to BCP coordinators on the results. In our review of a sample of BCPs we found that improvements to the review process are required and that more feedback should be provided to the BCPCs. A review by a single individual is not sufficient; a review by a committee or a group established for such a purpose would be better.

A key requirement of the TBS *Operational Security Standard - Business Continuity Planning (BCP) Program* is the regular testing of BCPs. BCPs are not considered complete until they have been tested, results of the testing documented, and revisions made as a result of the testing process. There are various degrees of testing, ranging from a walk-through by the recovery team to more elaborate testing using alternate facilities. BCPs in the Department of Justice have not been tested. Comprehensive tests that simulate major disruptions and require the use of alternate facilities are needed. The DBCPC does not formally monitor BCP testing but we were told he is aware of the need. IMB management told us that it plans [Text Removed]

PSEPC distributed a Quick Scan questionnaire in December 2005 to all government departments as part of an initial assessment of the BCP programs. The questionnaire consisted of 17 questions addressed to DMs. The questions required one of two responses: whether a requirement was met or not met. The questionnaire did not allow for answers with respect to partially met requirements. The Department answered that all requirements were met [Text Removed]

Because of the limited response options in the Quick Scan questionnaire, the results do not accurately reflect the status of BCPs in the Department. The impact of these results is twofold: the DM has not been provided with accurate information and PSEPC has acquired an inaccurate impression of the status of BCPs in the Department.

The BCP program of the Department is well regarded by TBS. For example, the DBCPC has been invited to give presentations on business continuity planning to other government departments and foreign visitors. We note, however, that TBS has not requested nor assessed the BCPs of the Department.

Recommendations and Management Response

10. It is recommended that the ADM, Corporate Services ensure that:

- a) A more thorough yearly review of BCPs is undertaken, feedback is provided to BCPCs, and BCPs are revised as required.**

Agree. At the end of the 2007-08 update cycle, a consolidated written report will be prepared and disseminated to all CBCPs with requests for further updates as necessary.

- b) BCPs are tested regularly, a formal report on test results is prepared, and BCPs are revised as required.**

Agree. Completion date and full testing of all BCPs will heavily rely on the provision of extra human and financial resources.

- c) The DM is advised of the limitations of the responses to the Quick Scan questionnaire.**

Agree. Will require discussion with PSEPC who advised Justice on the completion of this Quick Scan Document. As this is a PSEPC document, they will be encouraged to advise all Deputy Ministers of the limitations of their questionnaire.

4. FINDINGS—BACKUP PROVISIONS

Backup processes for IT data and software are generally appropriate. Usually, there is off-site backup of data and software each night. However, we found some deficiencies. We were told that one regional office has weekly and not daily off-site backup, which could result in the loss of up to five days of data. Also, some backup sites are located within close proximity of the primary site. [Text Removed] It is unclear to us whether copies of all required computer documentation, application source code, and original software media are kept off-site.

We found that off-site hardware backup to meet recovery requirements is also insufficient and has not been tested to ensure essential services recovery in case of disaster. Also, there are no documented plans for obtaining the backup hardware when it is needed. [Text Removed]

A report was prepared in 2006 for Family Orders and Agreements Enforcement Assistance (FOAEA) that recommended a hot (ready-to-function) backup alternate site for its application system. [Text Removed]

IMB staff have discussed the capacity for sites in different cities to back up each other's hardware but no plan has been developed. The main impediment is that funding is not assigned for the purchase and maintenance of alternate IT equipment. The Department must assess and determine how much equipment it will need. In the event of a wide-ranging disaster, it may take a long time to obtain replacement equipment, as many federal government institutions and private industry companies will have similar requirements. IMB management advised us that they decided not to contract with suppliers to replace equipment in the event of a disruption due to cost considerations and the low risk. IMB management is of the view that other institutions such as PSEPC, PWGSC, and TBS would assist if required. In our view, the BCPs need to more clearly document recovery limitations.

Except for IMB's BCP, other headquarters BCPs do not have written agreements or MOUs for the use of alternate backup facilities.

Recovery kits that are stored at alternate sites can facilitate recovery. These kits contain copies of essential records and references, the BCP (in paper and electronic removable media formats),

necessary forms (for urgent financial, human resources, administrative, legal, and other essential business), and any other items that may facilitate business continuity. Some BCPCs have prepared or are in the course of preparing basic recovery kits. [Text Removed] We were told that IMB staff intend to prepare recovery kits with electronic removable media and procedures to start up the backup servers, WAN, and applications, and to recover the required data and software. This could save 12 to 24 hours in the recovery process.

Recommendations and Management Response

11. It is recommended that the ADM, Corporate Services in collaboration with the senior regional directors ensure that:

a) Backup media is taken off-site each day.

Agree. IMB will undertake the necessary actions to ensure that backup media is taken off-site at an appropriate frequency, commensurate with the volume, sensitivity and volatility of data at risk.

b) Backup media is stored an appropriate distance away from the primary facility and in locations with continuous ready access.

c) Managers are aware of the recovery limitations of backup hardware.

d) The recovery procedures of BCPs are adjusted in accordance with current backup hardware limitations.

e) Written agreements or MOUs are prepared with those organizations that will provide backup facility sites.

f) Recovery kits are prepared, referred to in BCPs, and stored at alternate sites.

Agree. IMB will ensure that all recommendations (b to f) are implemented, on a national basis, during FY 2007/08.

5. FINDINGS—POST-MORTEM REPORTS

Post-mortem reports identify issues and ensure that needed improvements are made to BCPs. We found that post-mortem reports have not been prepared for all situations in which BCPs were used or operations were interrupted (e.g. a computer virus occurrence and loss of power in part of a building in one RO). A comprehensive post-mortem report was prepared after the August 2003 power failure that affected large parts of Ontario including Ottawa and Toronto. Following the post-mortem report, some improvements were made to the BCP and others were planned. However, there is no formal follow-up status report that indicates the resolution of the issues identified in the post-mortem report. In those situations in which post-mortem reports are not prepared, important opportunities to improve BCPs are missed.

Recommendations and Management Response

12. It is recommended that the ADM, Corporate Services ensure that following interruptions in operations:

a) Post-mortem reports are prepared to identify issues.

Agree. Post mortem reports are produced as warranted by emergency situations requiring such reports.

b) A formal follow-up status report is prepared to ensure that issues have been appropriately addressed.

Agree. Formal follow-up status reports to ensure issues have been appropriately addressed will be produced as required.

6. FINDINGS—SECURITY IN EMERGENCY AND INCREASED THREAT SITUATIONS

BCPCs are well aware of the requirement to maintain security at all times including when implementing business continuity plans. However, a security issue arises when private homes are used as alternate sites during a disruption. We discuss this issue in “Content and Clarity of BCPs” and make a recommendation.

7. FINDINGS—LEGAL SERVICES UNITS

Approximately 40 LSUs offer essential services to clients. We were told that in the event of a disaster or other interruption at their primary facilities, they must continue to provide some services within hours or at the most one day. LSUs are supported by the client department and the Department of Justice. The client provides office services (e.g. office space, IT services, support staff, telephone), while the Department of Justice provides expert legal advice to the LSU and access to departmental e-mail addresses. Furthermore, the Department provides access to:

- iCase
- PeopleSoft
- Salary Management System (SMS)
- Integrated Financial and Materiel System
- Records Information Management System
- Legal Opinions and Precedents On-line Retrieval System (LOPORS) and other legal research information and systems (Some LSUs use LOPORS to store their local records.)

The Department of Justice takes the position that LSUs are covered by the BCPs of the client departments and there is no need for it to take further action. The Department has provided no guidance to LSUs with respect to business continuity planning and has no knowledge of the status of BCPs in LSUs. Furthermore, there are no BCPs for the services that the Department provides to LSUs. In our interviews LSUs indicated that they require BCP support from the Department. Most LSUs we interviewed have little knowledge of BCPs. Yet the post-mortem report prepared by the Department after the August 2003 power failure in Ontario stated the need to include LSUs in the BCPs of the Department. Our interviews also indicated that some BCP coordinators understand the need to include LSUs in their BCPs. The Emergency Plan refers to LSUs but primarily from the point of view of keeping them informed of the Emergency Plan. It also states: “LSUs are included in their host departments’ Emergency Plans. An incident that affects an LSU’s host department may not affect the Department of Justice directly. However, the Senior Management Board (SMB) may direct the EMC to assist the LSU in order that it can continue to deliver its essential functions.” The Emergency Plan does not directly address

business continuity planning for LSUs. *A Guide to Business Continuity Planning in the Department of Justice* also does not refer to LSUs.

IMB staff informed us that they have discussed the need to provide services to LSUs in the event of a disruption. They also told us that the Department has good secure remote access, which is available to LSUs and is used by some staff. However, the potential use of this remote access for BCP purposes has not been analyzed nor documented.

Staff in LSUs generally do not have sufficient knowledge about business continuity planning. Few LSUs we contacted could provide us with copies of their BCPs, as most LSUs did not have copies of their BCPs readily available. We were told by staff from our sample of LSUs that each LSU has a BCP or that the LSU is covered by the client's BCP, but that none of these BCPs has been tested.

Recommendations and Management Response

13. It is recommended that the ADM, Corporate Services in collaboration with the CIO and the heads of LSUs, where appropriate, ensure that:

a) Department of Justice BCPs address the continuity of services provided by the Department to LSUs.

Agree. IMB will seek agreement from Bit.Com as to which level of continuity of service should be provided to DLSUs, in light of resources available, and will incorporate these services into its BCP during FY 2007/08.

b) LSUs receive training with respect to business continuity planning.

Agree. Work is currently underway to establish MOUs between the Department of Justice and client departments for the provision of LSU services. BCPs will be addressed in these MOUs.

8. FINDINGS—COMPLIANCE WITH GOVERNMENT POLICIES

The Department of Justice has made progress but needs to improve compliance, *as discussed throughout the report*, with departmental policies and standards, the *Government Security Policy*, the *TBS Operational Security Standard - Business Continuity Planning (BCP) Program*, and the *Operational Security Standard: Management of Information Technology Security (MITS)*, which assigns a high priority to BCPs.

9. RECOMMENDATIONS AND MANAGEMENT RESPONSE

1. It is recommended that the ADM, Corporate Services ensure that:15

a) A departmental business continuity planning policy is developed.

Agree. A departmental BCP policy has been completed and is pending management approval.

b) The authorities for the approval and activation of BCPs are clearly defined and documented.

Agree. Once the authority process has been approved by the EMC it will be clearly defined and documented.

c) The *Guide to Business Continuity Planning in the Department of Justice* is made more clear and consistent.

Agree. The guide will be updated along with other related documents.

d) The linkages between the Emergency Plan and BCPs (and related documents) are clarified and that related documents use common terms and include cross-references, where appropriate.

Agree. A thorough review and comparison of these documents will be conducted so as to reflect any applicable linkages. This could include the creation of glossaries and electronic links as well

e) The scope of BCPs is clarified in appropriate documents to reflect that BCPs deal only with the continuity of essential operations.

Agree. The scope will be reviewed and clarified by the EMC and documented as appropriate.

2. It is recommended that the ADM Corporate Services ensure that:.....17

- a) A committee or group is formed to review all BCPs and all substantive changes to BCPs.**

Agree. The formation of such a committee will be reviewed and discussed by the current Emergency Measures Committee and a decision will be made as to the structure of this new committee.

- b) The Emergency Measures Committee is reactivated and regular meetings are held.**

Agree. The EMC was reactivated and convened for a roles and responsibilities refresher as well as a tabletop exercise in June of 2006.

- c) Members of the EMC are trained in their role with respect to business continuity planning.**

Agree. BCP training was addressed in the form of “what if” scenarios and members were tasked with assisting in the rewrite of the Departmental Emergency Plan.

- d) The BCP responsibilities of key managers who provide common services to a region or to the Department as a whole are clarified.**

Agree. Key managers will be assembled to address this issue and documentation to clarify their position.

- e) The need for coordination among BCPCs is reflected in their responsibilities.**

Agree. Training sessions are being planned for all BCPCs for the Spring of 2007.

3. It is recommended that the ADM, Corporate Services ensure that:.....19

- a) Threat and risk assessments are prepared that identify the business impact of not continuing certain functions and establish a complete and prioritized list of detailed functions, processes, and services that require continuity and recovery.**

Agree. TRAs will be conducted as required. A Security TRA at the national level is anticipated for FY 2007-08.

- b) A plan is documented and regularly updated that lists activities to be completed for the effective operation of the BCP program including a list of required BCPs, completion of pending BCPs, testing of all BCPs, and capability of BCPs to meet business continuity requirements.**

Agree. A document to accompany the current BCP Control Chart will be developed to further explain how the BCP Program runs and include all the benchmarks recommended.

- c) An umbrella BCP is prepared for Headquarters.**

Agree in principle. This will require discussion with PSEPC to determine parameters of this “umbrella” document given their lead role in government BCP preparation.

- d) The preparation of a Departmental Consolidated Business Continuity Plan is considered, where beneficial.**

Agree in principle. This will require discussion with PSEPC to determine need for “umbrella” plan and “consolidated plan”.

- e) Services provided to LSUs by the Department are considered in the threat and risk assessments and are included in BCPs as appropriate.**

Agree. Work is currently underway to establish MOUs between the Department of Justice and client departments for the provision of LSU services. BCPs will be addressed in these MOUs.

- f) A plan is prepared for the completion of pending BCPs.**

Agree. This will be completed by the departmental BCP coordinator in consultation with areas requiring plans.

- 4. It is recommended that the ADM, Corporate Services ensure that written reports related to the BCP Program are prepared and distributed.....21**

Agree. A written report will be provided to the ADMCS monthly.

5. It is recommended that the ADM, Corporate Services request that:22

- a) BCP coordinators spend the appropriate time on necessary activities to complete BCPs.**

Agree. Timing, implementation and control will be discussed and decided by the EMC.

- b) A trained backup staff member is assigned for each BCPC.**

Agree. We strongly recommend the requirement for a trained backup BCPC for each plan although most already have one and are documented as such in their plans. This recommendation will be addressed in an annual BCP update reminder from the office of the ADMCS and will request a list of backups which will be trained by their respective BCPCs and SOTAD.

6. It is recommended that the ADM, Corporate Services ensure that the specified recovery times take into account departmental capacity to meet them and that recovery options and costs are prepared and presented to management.22

Agree. Will require discussion with PSEPC to determine current framework for this information to be expressed to management.

7. It is recommended that the ADM, Corporate Services ensure that:.....25

- a) Coordination of the activities of the BCPCs is improved.**

Agree. This will happen throughout 2007-08 as the BCP Program plans are updated.

- b) The departmental Emergency Plan is distributed to BCPCs.**

Agree. To be distributed once it has been updated and finalized.

- c) BCPs include clear linkages to building emergency plans.**

Agree. The scope of all BCPs will be reviewed to ensure appropriate linkages are in place once the Departmental Emergency Plan has been reviewed, updated and approved by the Emergency Measures Committee.

- d) Coordination among those Headquarters managers who play a key role in business continuity and recovery of normal operations is improved.**

Agree. To improve coordination, common issues will be identified by the departmental BCP Coordinator who will meet with the managers as appropriate.

- e) A list of hardware and software requirements should be listed in BCPs or in System Start-up Kits.**

Agree. IMB plans to have this addressed in recovery kits for critical systems during FY 07/08. In order to minimize data maintenance problems and errors, this list will only be included in application specific recovery kits.

- f) BCPs document the established arrangements with key suppliers and government departments that provide services in support of business continuity for the Department.**

Agree. BCPCs will be advised to document this information as their plans are updated.

8. It is recommended that the ADM, Corporate Services ensure that:.....27

- a) A list is maintained to indicate which BCPCs have received training.**

Agree. The departmental BCP Coordinator will develop and maintain this list. The annual update memo will address training requirements.

- b) Training is provided to BCPCs who have not received training.**

Agree. To the extent possible as we need to be regularly informed of staff changes. Annual memo will address training requirements.

- c) BCPCs are encouraged to refer to the information contained on the Security Web site that relates to business continuity planning.**

Agree. A note to reflect this will be added to regular BCP update memos.

9. It is recommended that the ADM, Corporate Services ensure that:.....31

- a) The terminology used in BCPs is reviewed and clarified and their organization is improved.**

Agree. A thorough review and comparison of these documents will be conducted by the departmental BCP Coordinator so as to clarify their organization and the terminology used.

- b) The template used for preparing BCPs is revised.**

Agree. Discrepancies or variances from standard or approved templates will be reviewed and our templates will be revised as necessary.

- c) All important information is included in BCPs.**

Agree. PSEPC will be consulted to determine what requirement Justice BCPs are missing.

- d) Recovery times specified in BCPs are consistent within each BCP and substantiated.**

Agree. BCPCs will be advised to substantiate recovery times as they update their plans.

- e) The scope of BCPs regarding the time period or activities they cover is clearly and consistently defined in the Emergency Plan, the *Guide to Business Continuity Planning in the Department of Justice*, and the BCPs.**

Agree. The scope will be clearly defined in all BCPs and associated plans and guides.

- f) The transition to normal operations is documented and linked to BCPs.**

Agree. Will require discussion with PSEPC.

- g) The following are documented in BCPs: any limitations, results of testing, arrangements with suppliers or other organizations, backup facilities and required equipment.**

Agree. The departmental BCP Coordinator will ensure that this information is documented in all BCPs as they are updated.

- h) The departmental requirements and conditions including security considerations for the use of private homes with respect to business continuity planning are documented.**

Agree. Will require discussions with PSEPC to verify requirements.

- i) Any additional procedures for business continuity that are currently not part of the BCPs are included or referred to in the BCPs.**

Agree. CBCPs will be reminded to include such documentation as part of the annual BCP reminder memo.

- j) The document on “Business Continuity with respect to Human Resources Matters” issued by TBS is included, summarized, or referred to in the BCPs.**

Agree. CBCPs will be advised of this document as they are reminded of their annual updates. The document will also be referred to in the annual BCP update memo.

10. It is recommended that the ADM, Corporate Services ensure that:.....34

- a) A more thorough yearly review of BCPs is undertaken, feedback is provided to BCPCs, and BCPs are revised as required.**

Agree. At the end of the 2007-08 update cycle, a consolidated written report will be prepared and disseminated to all CBCPs with requests for further updates as necessary.

- b) BCPs are tested regularly, a formal report on test results is prepared, and BCPs are revised as required.**

Agree. Completion date and full testing of all BCPs will heavily rely on the provision of extra human and financial resources.

- c) The DM is advised of the limitations of the responses to the Quick Scan questionnaire.**

Agree. Will require discussion with PSEPC who advised Justice on the completion of this Quick Scan Document. As this is a PSEPC document, they will be encouraged to advise all Deputy Ministers of the limitations of their questionnaire.

11. It is recommended that the ADM, Corporate Services in collaboration with the senior regional directors ensure that:.....36

a) Backup media is taken off-site each day.

Agree. IMB will undertake the necessary actions to ensure that backup media is taken off-site at an appropriate frequency, commensurate with the volume, sensitivity and volatility of data at risk.

b) Backup media is stored an appropriate distance away from the primary facility and in locations with continuous ready access.

c) Managers are aware of the recovery limitations of backup hardware.

d) The recovery procedures of BCPs are adjusted in accordance with current backup hardware limitations.

e) Written agreements or MOUs are prepared with those organizations that will provide backup facility sites.

f) Recovery kits are prepared, referred to in BCPs, and stored at alternate sites.

Agree. IMB will ensure that all recommendations (b to f) are implemented, on a national basis, during FY 2007/08.

12. It is recommended that the ADM, Corporate Services ensure that following interruptions in operations:39

a) Post-mortem reports are prepared to identify issues.

Agree. Post mortem reports are produced as warranted by emergency situations requiring such reports.

b) A formal follow-up status report is prepared to ensure that issues have been appropriately addressed.

Agree. Formal follow-up status reports to ensure issues have been appropriately addressed will be produced as required.

13. It is recommended that the ADM, Corporate Services in collaboration with the CIO and the heads of LSUs, where appropriate, ensure that:.....44

a) Department of Justice BCPs address the continuity of services provided by the Department to LSUs.

Agree. IMB will seek agreement from Bit.Com as to which level of continuity of service should be provided to DLSUs, in light of resources available, and will incorporate these services into its BCP during FY 2007/08.

b) LSUs receive training with respect to business continuity planning.

Agree. Work is currently underway to establish MOUs between the Department of Justice and client departments for the provision of LSU services. BCPs will be addressed in these MOUs.