National Defence / Défense nationale

Department of National Defence
Canadian Forces

LEVEL 0
BUSINESS CONTINUITY PLAN

"Ensuring Defence Mission Success in Times of Crisis"

January 2010

This page intentionally left blank.

Table of Contents

March 2010

DND/CF L0 BUSINESS CONTINUITY PLAN

1. The Policy on Government Security requires departments to establish a Business Continuity Planning Program (BCPP) to provide for the continued availability of critical services and their associated assets. Critical services are those which, if disrupted, are likely to cause a high degree of injury to the health, safety, security or economic well-being of Canadians, or to the efficient functioning of the Government of Canada. In the context of the *Canada First* Defence Strategy, DND/CF play a unique role in ensuring public confidence in the government's ability to respond in times of crisis.

2. DND/CF have a mandate to support the government with confidence to carry out missions ranging from search and rescue, to humanitarian assistance, to domestic crisis response, to work alongside law enforcement agencies; and provide support to other government departments on challenges as diverse as drug interdiction, human trafficking and over-fishing. Our members are deployed around the globe, bringing Canadian values to international operations aimed at improving worldwide stability.

3. When critical services and operations, and their associate assets, cannot be delivered, consequences can be severe. All organizations are at risk and face potential disaster if unprepared. The Business Continuity Plan is a tool that not only allows the organization to mitigate risks, but to ensure the continued delivery or timely restoration of critical services and operations despite disruption.

4. Since the issuance of a DM/CDS Initiating Directive on Business Continuity Planning (Continuity of Operations) on 5 January 2007, a great deal of progress has been made on the DND/CF BCPP. The BCPP is an evergreen program which will continue to undergo development in future years. Given the scope of DND/CF services and operations, their organizational size and complexity, and the many interdependencies between organizations, it is recognized that there will be gaps that will surface. The DND/CF L0 BCP provides a sound framework to mature the program and address these gaps in order to ensure Defence mission success in times of crisis.

J.A.D. Rouleau
Vice-Admiral
Vice Chief of the Defence Staff

EXECUTIVE SUMMARY

In accordance with the Policy on Government Security (PGS), all departments must establish a Business Continuity Planning (BCP) Program to provide for the continued availability of services and associated assets that are critical to the health, safety, security and economic well-being of Canadians, or the effective functioning of government. Creating and maintaining a BCP helps ensure that an organization has strategies, processes and procedures to restore critical services and operations following a traumatic event, emergency or disruption. Within the Government of Canada (GoC), the Treasury Board Secretariat is responsible for the over-arching policies related to BCP Programs, while Public Safety Canada is responsible for ensuring and validating that departments are complying with the PGS.

The Department of National Defence and the Canadian Forces Business Continuity Plan (DND/CF BCP) has been prepared under the direction of the Deputy Minister (DM) and Chief of the Defence Staff (CDS). The Assistant Deputy Minister (Finance and Corporate Services) (ADM (Fin CS)) and the Director of Staff Strategic Joint Staff (DOS SJS) are jointly responsible for the preparation, exercise and maintenance of the DND/CF BCP Program. This responsibility is exercised through a BCP Action Team co-chaired by the Director General Corporate and Shared Services from ADM (Fin CS) and the Director General Plans from the SJS. The BCP Action Team has a Director-level representative from each Level 1 organization as well as key representatives, e.g. Departmental Security Officer.

The L0 DND/CF BCP applies to all organizations within DND/CF. The purpose of the Plan is to outline the processes and procedures to be used to respond, recover and restore DND/CF critical services and operations to minimum levels following a traumatic event, emergency or disruption. In addition, Defence portfolio organizations are also undertaking to develop their own BCPs, in conjunction with the DND/CF BCP Program. These organizations are:

a. The National Search and Rescue Secretariat;
b. Communications Security Establishment Canada (CSEC);
c. The Office of the Commissioner of CSEC;
d. The Military Police Complaints Commission;
e. The Chief Military Judge;
f. The Canadian Forces Grievance Board;
g. Defence Research and Development Canada; and
h. The National Defence and Canadian Forces Ombudsman.

The DND/CF BCP Policy can be found in Defence Administrative Orders and Directives 1003-0 - Business Continuity Planning and 1003-1 - Business Continuity Planning Program. The BCP Policy details the DND/CF BCP governance structure. This governance structure establishes clear lines of authority, accountability and responsibility, and will ensure that DND/CF is well prepared to respond to an emergency or a disruption, thereby facilitating a rapid recovery and restoration of DND/CF critical services and operations.

The DND/CF Threat and Risk Assessment (TRA) identified a wide variety of events that could affect DND/CF services and operations. These events can be categorized as resulting in:

a. Loss of staff, e.g. due to a Pandemic Influenza;
b. Loss or disruption of services, e.g. electricity or network services; and/or
c. Loss or disruption to facilities, e.g. fire or physical attack.

The DND/CF Business Impact Analysis (BIA) has identified the Maximum Allowable Downtime and Minimum Service Levels of DND/CF critical service and operation at Level 0 and Level 1 and is classified SECRET. Both the TRA and the BIA can be found on the secure DND/CF network, under ***TITAN (CSNI)/Comd-Net Home Page/Corporate/Business Continuity Planning/BIA/DND-CF Level 0/.***

The strategic level DND/CF critical services and operations can be grouped into four categories, the first three of which are derived from the Canada First Defence Strategy:

a. Defend Canada;
b. Defend North America;
c. Contribute to International Peace and Security; and
d. Continuity of the Constitutional Government.

DND/CF abilities to deliver its critical operations are reliant upon the continued delivery of certain internal and external dependencies. The Concept of Operations for BCPs at all levels must take into consideration how these dependencies will be met/delivered or else provide mitigation strategies to ensure continuity of critical services and operations while partner organizations restore such services. These dependencies can generally be categorized as:

a. Internal Dependencies:
    i. Facilities;
    ii. Personnel;
    iii. Command and Control;
    iv. Decision Support; and
    v. Support/Sustainment.

e. External Dependencies:
    i. Safety – i.e. first responders;
    ii. Services – electricity, gas, oil, water;
    iii. Communications – network providers;
    iv. Facility Management – service and maintenance; and
    v. External suppliers and shippers.

PLAN IMPLEMENTATION

The following assumptions have been made in the development of the DND/CF BCP:

a. A significant disruption will affect DND/CF services and operations;
b. The planning period for BCP is the first 30 days of a disruption;
c. Key personnel (or their succession) will be available; and
d. Alternate DND/CF national command centres will be available.

The DM/CDS intent for the BCP Program states: “The capability of DND/CF to support the effective functioning of government and the continued pursuit of GoC objectives, both at home and abroad must continuously be maintained. This means we must be prepared, in any circumstance, to continue to conduct critical operations and deliver critical services whilst recovering quickly from the effects of natural or human-induced trauma. Redundancies, alternate arrangements and effective Departmental strategies must be in place and regularly exercised to ensure the continuity of critical operations and the uninterrupted delivery of critical services.”

The DND/CF BCP can be described as progressing through four phases:

a. *Phase 1 - Mitigation and Prevention*. Mitigation plans and controls eliminate or reduce threats and hazards that can impact operations. Key aspects are ensuring personnel safety, physical security of facilities, systems integrity and records management;
b. *Phase 2 – Response to a Disruption*. DND/CF actions to be taken during a crisis, emergency or a disruption include assessing the situation, reporting damage to the CFICC, activating alternate facilities as necessary, populating details of the incident on the CSNI Incident Management System, notifying and briefing the DM, CDS and Level One senior leaders as required, activating BCP(s) as required and, throughout, communicating with employees, partners and the public;
c. *Phase 3 – Recovery*. Re-establishing critical services and operations as directed by DND/CF executive authorities (DM/CDS); and activating DND/CF recovery plans (e.g. IT/IM continuity) to ensure Minimum Service Levels are maintained and Maximum Allowable Downtimes are respected; and
d. *Phase 4 – Restoration*. Re-establishing all DND/CF services and operations to normal levels.

In the event of a disruption, information will be provided to the DM and CDS as expeditiously as possible; using whatever means (e.g. briefings, telephone, e-mail) are appropriate. The initial information requirements of the DM and CDS during a disruption of service are:

a. the nature and scale of the disruption;
b. the impact the disruption will have on DND/CF operational capability and readiness; and
c. the effect on DND employees and CF members.

BCP readiness includes continuous maintenance, change management, training employees and other persons, exercising, preparing lessons learned reports and updating plans when there is a change in personnel, process, technology or departmental structure. The DND/CF BCP will be updated on an iterative basis to enable the Department to anticipate new risks and develop measures to address these risks. BCP Program documentation should be revised every time there is a change to the organization that has an impact on the BCP.

BCP Program Documentation will be held by the BCP Secretariat and updated versions will be required to be reviewed and re-submitted at least annually or whenever a significant organizational change occurs that would prompt a review and revision of a BCP document.

Testing and validating the BCPs will be done on a regular basis, with a Level 0 exercise conducted at a minimum every two years.

Numerous plans, programs and strategies form an integral part of the DND/CF BCP program. The following additional Annexes cover other aspects to the BCP plan and provide direction for review and refinement of Level 0 and Level 1 BCPs:

ANNEX A – Response and Recovery Strategies – Offices of Senior Leadership (SECRET)
ANNEX B – DND/CF BCP IM/IT Recovery Plan
ANNEX C – DND/CF Pandemic Influenza Plan
ANNEX D – DND/CF Accommodations Plan relating to BCP
ANNEX E – CF Succession of Command and Alternate Command Centre Plan
ANNEX F – Instructions on maintaining BCP Contact List
ANNEX G – DAODs 1003-0 and 1003-1
ANNEX H – DND/CF BCP Response Management Process
ANNEX I – DND/CF BCP Communications Strategy
ANNEX J – DND/CF BCP Exercise Strategy
Appendix 1 – NCR Exercise Scenarios
ANNEX K – Key References
ANNEX L – Glossary

PLAN MAINTENANCE

The Department of National (DND)/Canadian Forces (CF) Business Continuity Plan (BCP) and accompanying annexes will be updated as required. Specifically, maintenance entries will record:

- The conduct of plan reviews and exercises; and
- Changes to organizational structures and/or functional responsibilities.

Recommended changes should be forwarded to the DND/CF BCP Lead Planners.

BUSINESS CONTINUITY PLAN AMENDMENT HISTORY			
Change #	Date	Brief Description and Page Reference	Authorized By

This page intentionally left blank.

PART ONE - OVERVIEW

INTRODUCTION

1. Every organization is at risk from potential disruptions resulting from:

   a. Natural disasters such as tornadoes, floods, blizzards, earthquake and fire;

   b. Power and energy disruptions;

   c. Communications, transportation, safety and service sector failures;

   d. Environmental accidents causing facility contamination;

   e. Cyber attacks and hacker activity; and

   f. Physical attacks.

2. In accordance with the Policy on Government Security (PGS), all departments must establish a Business Continuity Planning (BCP)[1] Program to provide for the continued availability of services and associated assets that are critical to the health, safety, security and economic well-being of Canadians, or the effective functioning of government. Creating and maintaining a BCP helps ensure that an organization has a strategy, processes and procedures to deal with these emergencies.

PURPOSE

3. The purpose of this plan is to outline the processes and procedures to be used to respond, to recover and restore DND/CF critical services and operations to minimum levels following a traumatic event, emergency or disruption.

AUTHORITY

4. The DND/CF L0 BCP has been prepared under the direction of the Deputy Minister (DM) and Chief of the Defence Staff (CDS). The Assistant Deputy Minister (Finance and Corporate Services) (ADM (Fin CS) and the Director of Staff Strategic Joint Staff (DOS SJS) are jointly responsible for the preparation, exercise and maintenance of the DND/CF BCP Program.

APPLICABILITY

5. This Level 0 BCP applies to all organizations within the Department of National Defence (DND) and the Canadian Forces (CF).

[1] In this plan, the abbreviation BCP refers to both Business Continuity Planning and Business Continuity Plan depending on the context.

KEY DEFINITIONS AND REFERENCES

6. A list of key references and glossary of BCP terms can be found at annexes K and L respectively. The following key definitions will be used throughout this plan:

a. **Business Continuity Planning (BCP)** is an all-encompassing term which includes the development and timely execution of plans, measures, procedures and arrangements to ensure minimal or no interruption to critical operations and the continued availability of DND/CF critical services and operations, and associated assets;

b. **Critical Operations and Services** are DND/CF activities whose compromise in terms of availability or integrity would result in a high degree of injury to the health, safety, security or economic well being of Canadians, or to the efficient functioning of the Government of Canada (GoC). A BCP program assures that minimum service levels are maintained for critical operations and services; and

c. **Business Impact Analysis (BIA)** is the process of analyzing the degree to which DND/CF is exposed to risks, and impacts that could affect its ability to function, or its ability to provide the continuous delivery of critical services.

GOVERNMENT OF CANADA LEAD DEPARTMENT RESPONSIBILITIES

7. Within the GoC, the Treasury Board Secretariat (TBS) is responsible for the over-arching policies related to BCP Programs, while Public Safety Canada is responsible for ensuring and validating that departments are complying with the PGS. GoC Central Agencies, such as TBS and Public Works and Government Services Canada (PWGSC), have government-wide roles, responsibilities and authorities and can issue directives that apply to all government departments and agencies, including DND/CF. Directives issued by the above must be adhered to and taken into account when developing and/or invoking BCPs.

NATIONAL POLICY OBJECTIVES

8. In accordance with the PGS, the continued delivery of critical government services must be assured. The GoC BCP Program (BCPP) is designed to protect the resources on which the government relies. The objective of the GoC BCPP is:

> "To provide for the continued availability of services and associated assets that are critical to the health, safety, security or economic well-being of Canadians, or the effective functioning of government."

9. The GoC BCPP complements emergency preparedness that is mandated by legislation or government policy (e.g. fire and building evacuation plans; civil emergency plans).

DND/CF BCP POLICY

10. The DND/CF BCP policy states that:

> "The DND and the CF are committed to ensuring the continuity of critical operations and the continued availability of DND and CF critical services and associated assets in the event of any disruption of domestic, continental or international activities."

11. The policy requires that the DND/CF shall:

- Institute and maintain a BCP Program as a component of the *National Defence Security Policy*;
- Establish protocols and understandings with appropriate organizations to assist with the continuity, response and recovery efforts of the DND and the CF;
- Integrate the fundamentals of BCP into the decision-making process for capability development and program design;
- Articulate and communicate responsibilities to ensure that the BCP roles of DND employees and CF members are clearly defined and understood in BCPs;
- Ensure that the BCP Program policy, procedures and equipment, including software, are interoperable with other appropriate organizations to the greatest extent practicable;
- Ensure appropriate BCP training is provided as necessary to DND employees and CF members; and
- Provide a system of accountability to report deficiencies and vulnerabilities through the appropriate chain of command in order to initiate and adopt appropriate corrective measures.

12. The DND/CF BCP Policy can be found in Defence Administrative Orders and Directives 1003-0, Business Continuity Planning and 1003-1, Business Continuity Planning Program (see Annex G).

METHODOLOGY

13. The diagram at Figure 1 illustrates the methodology used to implement the BCP Program within DND/CF.

BCP Methodology

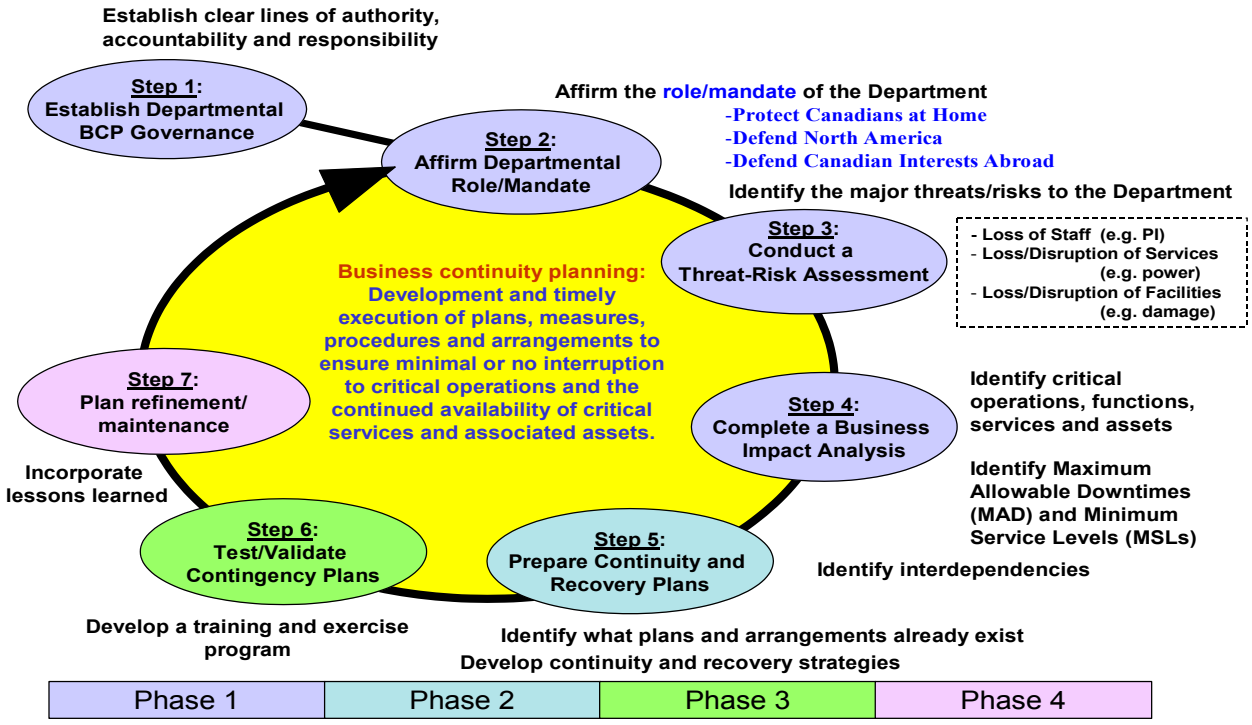

Figure 1 – DND/CF BCP Methodology

ROLE AND MANDATE OF DND/CF

14. The role and mandate of the DND/CF is:

a. **Defending Canada** - *ensuring the security of Canadians and helping exercise Canada's sovereignty;*

b. **Defending North America**– *being a strong, reliable partner to the United States in the defence of the continent*; and

c. **Contributing to International Peace and Security**– *projecting leadership abroad by making a meaningful contribution to international operations*.

15. The DND/CF is responsible to:

a. Provide strategic defence and security advice to the GoC;

b. Conduct surveillance and control of Canada's territory, airspace and maritime areas of jurisdiction;

c. Respond to requests from provincial authorities for *Aid of the Civil Power*;

d. Participate in bilateral and multilateral operations with Canada's allies;

e. Assist Other Government Departments and other levels of government in achieving national goals;

f. Provide support to broad federal government programs; and

g. Provide emergency humanitarian relief.

OVERVIEW OF DND/CF ORGANIZATIONAL ELEMENTS

16. **The Defence Portfolio.** The Defence Portfolio comprises DND, the CF and a number of unique organizations with federal responsibilities, all of which are the collective responsibility of the Minister of National Defence (MND). Together, the diverse elements of the Defence Portfolio provide the core services and capabilities required to defend Canada and Canadian interests, and form an important constituency within the broader Canadian national security community. Approximately 150,000 people are employed within the Defence Portfolio.

17. **DND.** The 'Department' of National Defence is established by a statute - the *National Defence Act* - which sets out the Minister's responsibilities, including the Minister's responsibility for the Department. The *Act* also stipulates that "there shall be a Deputy Minister of National Defence" who may exercise all of the Minister's powers, with the exception of matters that the Minister reserves for himself or herself; any case where contrary intention exists in legislation; and the power to make regulations. DND's relationship with the CF is that of an operations support system - as members of the Defence Team, civilian public servants work side by side with CF personnel to fulfill the Canadian government's mission to defend Canadian interests and values, and to contribute to international peace and security. DND is one of the largest federal departments in Canada, with approximately 30,000 civilian employees.

18. **The CF.** The CF is also established by the *National Defence Act* – which stipulates that the CF exists as an entity separate and distinct from the Department. The CF is headed by the CDS, who is Canada's senior serving officer and who, "subject to the regulations and under the direction of the Minister (is) ... charged with the command, control and administration of the CF". The *National Defence Act* stipulates that "unless the Governor-in-Council otherwise directs, all orders and instructions to the CF that are required to give effect to the decisions and to carry out the directions of the GoC or the Minister shall be issued by or through the CDS. CF personnel belong to air, land, maritime and special operations components, with approved manning levels numbering approximately:

a. 70,000 Regular Force members; and

b. 30,000 Reserve Force members, including 4,000 Canadian Rangers.

19. **Defence Portfolio Organizations with Federal Responsibilities.**

a. **National Search and Rescue Secretariat (NSS).** NSS acts as a liaison for Search and Rescue (SAR) agencies and all partners involved in Canadian search and rescue. The NSS has a separate BCP;

b. **Communications Security Establishment Canada (CSEC).** CSEC is a cryptology agency to collect foreign intelligence that can be used by the government for strategic warning, policy formulation, decision-making and day-to-day assessment of foreign capabilities and intentions. It produces intelligence reports based on electronic emissions and advises the government in the area of security for its telecommunications and automated information systems, foreign intelligence, as well assistance to federal law enforcement agencies. CSEC has a separate BCP;

c. **Office of the CSEC Commissioner.** The commissioner of CSEC, appointed by the Governor in Council, is responsible for reviewing the activities of the CSEC to ensure that they are in compliance with the law, undertaking any necessary investigation and to inform the Minister and the Attorney General of Canada of any activity of the CSEC that the Commissioner believes may not be in compliance with the law. The office of the Commissioner has a separate BCP;

d. **Military Police Complaints Commission (MPCC).** MPCC is established by the *National Defence Act* as an independent body responsible for examining complaints arising from either the conduct of military police members in the exercise of policing duties or functions or from interference in or obstruction of their police investigation. MPCC has a separate BCP

e. **Canadian Forces Grievance Board (CFGB).** CFGB is established by the *National Defence Act* as an impartial and independent body responsible for reviewing grievances submitted to it by the CDS, make conclusions and formulate recommendations. Article 7.12 of Queen's Regulations and Orders identifies the types of grievances that must be mandatorily referred to the CFGB. The CFGB has a separate BCP;

f. **The Office of the National Defence and Canadian Forces Ombudsman.** The Ombudsman acts on behalf of the Minister of National Defence, independent of the chain of command, as a neutral sounding board, mediator and reporter on matters related to the Department and the Canadian Forces. The Office of the National Defence and Canadian Forces Ombudsman has a separate BCP;

g. **Defence Research and Development Canada (DRDC).** DRDC is responsible for ensuring that the Canadian Forces is technologically prepared and operationally relevant by providing scientific and technological advice, products and services. The DRDC BCP is part of the L1 ADM(S&T) BCP.

h. **Office of the Chief Military Judge.** The office of the Chief Military Judge is an independent unit of the Canadian Forces whereby Military Judges adjudicate at courts martial and other military proceedings. The Office of Chief Military Judge has a separate BCP.

20. **Defence Management System.** Management of Canada's Defence Program, military and civilian personnel, and Departmental and CF activities requires continuing close cooperation among staff, both military and civilian, at all levels. The Defence Management System, based on a codified framework of accountabilities and responsibilities, relies on approved Level 1[2] business plans for the implementation of the Defence Services Program. The high level organization is depicted in the chart at Figure 2, and the chart at Figure 3 provides an overview of DND/CF Level 0 and Level 1 organizational elements. Level 1 roles, responsibilities and accountabilities are detailed in the DM/CDS Directive on BCP and Defence Administrative Orders and Directives and the Organization and Accountabilities document (see Annex K – Key References).

Figure 2 – DND/CF Organization

[2] A Level 1 Advisor is a senior manager who has direct accountability to the DM/CDS and for whom the DM/CDS exercise full authority to assign and adjust tasks, goals and resources.

DND Level 0 and Level 1 Organizational Elements	
Level 0	Minister's Office
	Deputy Minister
	Chief of the Defence Staff
Level 1s equally responsible to the DM and the CDS	Vice Chief of the Defence Staff
	Assistant Deputy Minister (Information Management)
	Assistant Deputy Minister (Science and Technology)
	Chief of Review Services
	Assistant Deputy Minister (Public Affairs)
	Chief of Defence Intelligence *(under authority of the VCDS)*
Level 1's primarily responsible to the DM	Associate Deputy Minister
	Assistant Deputy Minister (Finance and Corporate Services)
	Assistant Deputy Minister (Policy)
	Assistant Deputy Minister (Material)
	Assistant Deputy Minister (Infrastructure and Environment)
	Assistant Deputy Minister (Human Resources – Civilian)
Level 1s primarily responsible to the CDS	Director of Staff – Strategic Joint Staff
	Chief of the Maritime Staff
	Chief of the Land Staff
	Chief of the Air Staff
	Chief of Military Personnel
	Commander Canada Command
	Commander Canadian Expeditionary Forces Command
	Commander Canadian Special Operations Forces Command
	Commander Canadian Operational Support Command
Special organizations directly responsible to the Minister or having special reporting relationships	Canadian Security Establishment Canada (CSEC)
	Office of the Commissioner of CSEC
	DND/CF Ombudsman
	Military Police Complaints Commission
	Chief Military Judge
	National Search and Rescue (SAR) Secretariat
	Defence Research and Development Canada (DRDC)
	CF Grievance Board
	DND/CF Legal Advisor (also responsible to the DM of the dept of Justice)
	Judge Advocate General
= *civilian position*	= *military position*

Figure 3 – DND Level 0 and Level 1 Organizational Elements

BCP GOVERNANCE IN DND/CF

21. The DND/CF BCP governance structure establishes clear lines of authority, accountability and responsibility. This will ensure that DND/CF is well prepared to respond to a disruption or emergency, thereby facilitating a rapid recovery and restoration of DND/CF operations and services. The DND /CF governance structure includes:

a. **Executive Authority.** The ADM(Fin CS) and DOS SJS are jointly responsible for the preparation, exercise and maintenance of the DND/CF BCP Program;

b. **Senior Management.** The NDHQ Coordination Committee (NC2), chaired by the Vice Chief of the Defence Staff (VCDS) reviews and approves all aspects of the DND/CF BCP Program;

c. **Senior Leadership**. ADM(Fin CS)/Director General Corporate and Shared Services (DGCSS) and SJS/Director-General Plans (DGP) serve as the co-chairs of the DND/CF BCP Action Team and provide corporate/CF leadership to the DND/CF BCP Program;

d. **BCP Coordinator(s).** Senior DND and CF BCP coordinators have been appointed and serve as lead planners for the DND/CF BCP Program;

e. **BCP Action Team.** All L1 organizations within DND/CF (Director level representative), as well as key representatives such as the Departmental Security Officer (DSO), are members of the DND/CF BCP Action Team; and

f. **BCP Working Groups.** Functional Level 1 working groups develop and implement the BCP Program within DND/CF.

Figure 4 – DND/CF BCP Program Governance

22. A detailed list of DND/CF BCP Program appointments and responsibilities can be found in Defence Administrative Orders and Directives 1003-0, Business Continuity Planning and 1003-1, Business Continuity Planning Program (see Annex G).

THREAT AND RISK ASSESSMENT (TRA)

23. The DND/CF Threat and Risk Assessment (TRA) identified a wide variety of events that could affect DND/CF critical services and operations. These events can be categorized as resulting in:

a. Loss of staff, e.g. due to a Pandemic Influenza;

b. Loss or disruption of services, e.g. electricity or network services; and/or

c. Loss or disruption to facilities, e.g. fire or physical attack.

24. The complete DND/CF TRA is classified SECRET. It can be found on the secure DND/CF network, under ***TITAN (CSNI)/Comd-Net Home Page/Corporate/Business Continuity Planning/BIA/DND-CF Level 0/Level 0 Threat Risk Assessment 6 Jun 07.***

BUSINESS IMPACT ANALYSIS (BIA)

25. **DND/CF Critical Services and Operations.** The following operations performed by the DND/CF have been identified as "departmental operations that are critical to the health, safety, security or economic well being of Canadians, or to the efficient functioning of the GoC," pursuant to the GSP:

DND/CF Critical Operations	
Defend Canada	Surveillance and Control of Canadian Sovereign Territory
	Search and Rescue
	Humanitarian Assistance/ Disaster Relief
	Aid of the Civil Power
	Assistance to Other Government Departments (OGD)
	Assistance to Law Enforcement
	Counter-Terrorism Operations
Defend North America	Aerospace Warning and Control (NORAD Agreement)
	Maritime Warning (NORAD Agreement)
Contribute to International Peace and Security	Evacuation of Canadians from Threatened Areas
	Expeditionary Operations
Continuity of the Constitutional Government	Strategic Defence and Security Advice to Government of Canada
	Assistance to Other Government Departments and other levels of government

Figure 5 – DND/CF Critical Operations

26. The complete DND/CF BIA including the Maximum Allowable Downtime (MAD) and Minimum Service Levels (MSL) of each DND/CF critical service or operation is classified SECRET. It can be found on the secure DND/CF network, under ***TITAN (CSNI)/Comd-Net Home Page/Corporate/Business Continuity Planning/BIA/DND-CF Level 0/Level 0 Critical Operations Table 6 Jun 07.***

27. **Internal Dependencies.** The internal dependencies of DND/CF have been identified as:

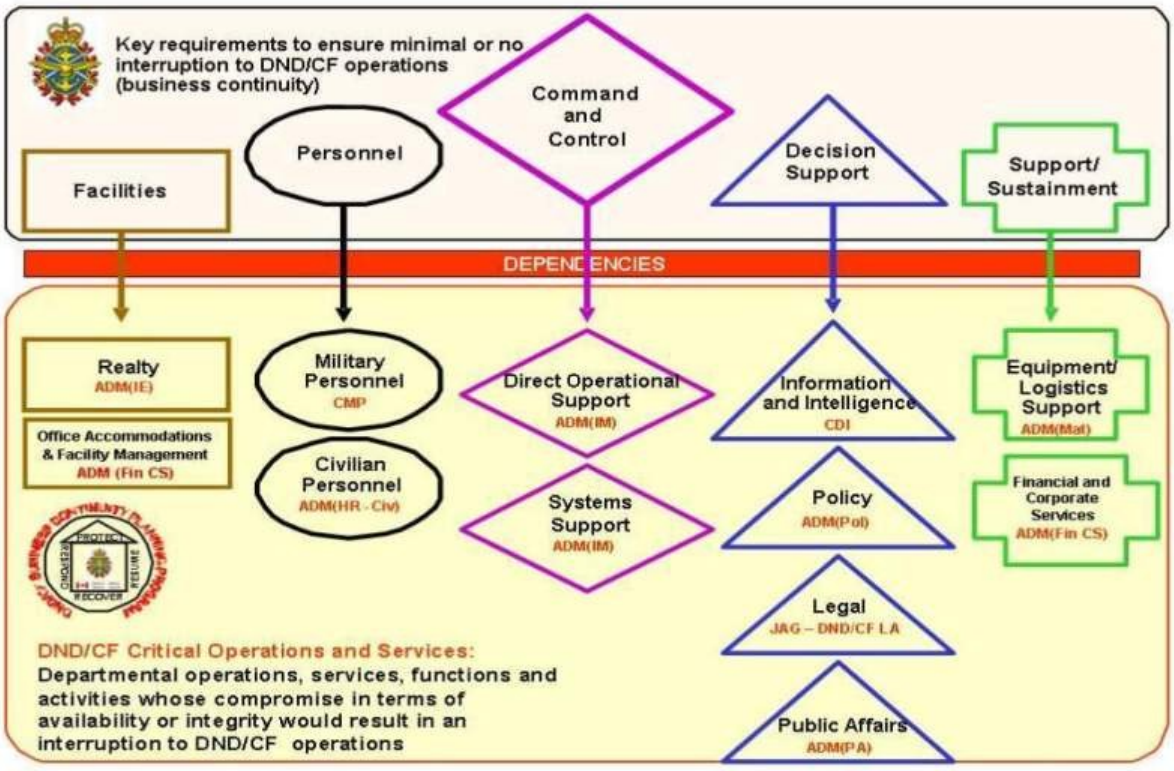

Figure 6 – DND/CF Internal Dependencies

28. **External Dependencies.** The external dependencies of DND/CF include, but are not limited to:

a. Safety – first responders, fire, police and ambulance;

b. Services – electricity, natural gas, oil, fuel, water;

c. Communications – network providers;

d. Facility management – service and maintenance; and

e. External suppliers and shippers.

29. **Critical Infrastructure.** Details on the DND/CF Critical Infrastructure Protection Program, including the identification of those “physical and information technology facilities, networks, services and assets which, if disrupted, would have a serious impact on the health, safety, security or economic well-being of Canadians or the effective functioning of government” is classified SECRET. Canada Command (Canada COM) and the Assistant Deputy Minister (Materiel) are the lead organizations within DND/CF for the identification of critical infrastructure.

PART TWO – PLAN IMPLEMENTATION

ASSUMPTIONS

30. The following assumptions have been made in the development of the DND/CF BCP:

a. A significant disruption will affect DND/CF critical operations and services;

b. The planning period for BCP is the first 30 days of disruption (BCP focuses on immediate concerns for the continued availability of critical operations/services);

c. Key personnel (or their succession) will be available; and

d. Alternate DND/CF national command centres will be available.

DM/CDS INTENT

31. The capability of DND/CF to support the effective functioning of government and the continued pursuit of GoC objectives, both at home and abroad must continuously be maintained. This means we must be prepared, in any circumstance, to continue to conduct critical operations and deliver critical services whilst recovering quickly from the effects of natural or human-induced trauma. Redundancies, alternate arrangements and effective Departmental strategies must be in place and regularly exercised to ensure the continuity of critical operations and the uninterrupted delivery of critical services.

DND/CF STRATEGIC OBJECTIVE

32. The DND/CF strategic BCP objective is to maintain DND/CF operational effectiveness and maintain CF readiness at near-full capacity for critical operations.

CONCEPT OF OPERATIONS

33. **DND/CF Recovery Strategy.** The DND/CF BCP recovery strategy addresses the key requirements of DND/CF to conduct critical services and operations, namely:

a. Facilities.

(1) An alternate site (national command centre) is to be maintained in “warm standby”;

(2) A clear order of succession of headquarters facilities (national through regional levels) has been established;

(3) Arrangements to ensure essential resources (electricity, communications, etc.) are to be in place;

(4) All organizations within DND/CF will identify alternate work sites for key staff; and

(5) All organizations will maintain arrangements to facilitate working from home combined with telecommuting where feasible.

b. Personnel.

(1) Notification and contact lists are to be maintained at all levels of DND/CF;

(2) Personnel mobilization plans are to be maintained;

(3) Operationally critical personnel are to be identified and advised;

(4) The roles and responsibilities of key individuals involved in BCP are to be defined;

(5) Arrangements to facilitate working from home during disruptions (e.g. Pandemic Influenza) are to be in place; and

c. Command and Control.

(1) Clear CF succession of command and DND lines of authority have been established;

(2) Authority has been delegated to operational and regional commanders to plan and conduct operations (decentralization of operations);

(3) Standard Operating Procedures (SOPs) are in place to manage a crisis, emergency or disruption within DND/CF;

(4) An incident management system is to be in place in DND/CF;

(5) A BCP Action Team has been created to ensure comprehensive BCP plans and arrangements are maintained;

(6) Functional DND/CF teams have been created to develop and maintain specific DND/CF plans and arrangements for critical DND/CF internal dependencies such as IT/IM continuity; and

(7) Web sites containing detailed information regarding the DND/CF BCP Program and the actions to be taken during a disruption have been established on secure and non-secure DND/CF networks.

d. Systems.

(1) Specific recovery and response plans are to be developed for:

(a) IT/IM continuity;

(b) Communications;

(c) Accommodations; and

(d) Vital Records;

(2) Redundancies in communication systems are to be in place (non-reliance on single systems/service providers); and

(3) Manual procedures will be maintained;

e. **Decision-Support.**

Arrangements and procedures are to be in place to ensure decision support (advice) to the MND, DM, CDS and other executive authorities are maintained during a disruption. DM and CDS hold significant regulatory and statutory authorities in responding to incidents. To ensure timely and informed decision making, as well as to ensure they are provided with proper and updated situational awareness, the following decision-support procedures apply:

(1) CDS – the CF Command and Control (C2) structure, with well defined areas of responsibility and established Operational Staff Procedures, ensure that issues are staffed-up to the CDS by the appropriate C2 authority and that advice/input has been previously sought from the relevant Level 1 organizations as required;

(2) DM – a Corporate Leadership Response Management Team has been established to provide decision support to the DM in the event of a significant disruption. This team is comprised of the following Level 1 advisors and can be activated by the DM, Assoc DM or ADM (Fin CS), as the DND Level 1 Authority for BCP:

(a) Assoc DM;
(b) ADM (Fin CS);
(c) DND/CF LA;
(d) ADM (Pol);
(e) ADM (Mat);
(f) ADM (IE);
(g) ADM (HR – Civ);
(h) ADM (PA); and
(i) A Military Liaison Officer from SJS;

(3) Level 1 organizations listed above will also appoint a Director General Level representative to a Senior Leadership Response Management Team. This team's purpose is to provide senior level advice when the incident is serious but does not require the active or direct involvement of the DM in response management or in planning a response to an emerging issue, such as an anticipated Pandemic Influenza. This team can be activated by ADM (Fin CS) or DGCSS as the DND Co-chair of the BCP Action Team ; and

(4) ADM (Fin CS)/DGCSS will coordinate the administrative support to these Response Management Teams.

f. **Sustainment.**

(4) Service-level agreements with vendors and suppliers during periods of disruption are to be maintained; and

(5) Alternate service delivery options during periods of disruption are to be maintained.

34. **Cooperation with OGDs and Partners.** In addition, DND/CF will examine mutual aid, reciprocal arrangements with other government departments and partners.

35. **DND/CF BCP Plan.**

a. **Phase 1. Mitigation and Prevention.** Mitigation plans and preventative controls eliminate or reduce threats and hazards that may impact the department. All organizations within DND/CF maintain plans, processes and procedures to ensure:

(1) Employee safety, e.g. emergency management plans for personnel evacuation during fires and other emergencies;

(2) Physical security of all facilities;

(3) Systems integrity; and

(4) Records management.

b. **Phase 2: Response to a Disruption.** DND/CF actions to be taken during a crisis, emergency or a disruption include:

(1) Assess the situation and report damage to the DND/CF Emergency Operations Center (CF Integrated Command Center);

(2) Activate alternate facilities as necessary (in accordance with DND/CF SOPs);

(3) Details of incidents/events are to be populated on the DND/CF Incident Management System located on the ***TITAN (CSNI)/ Comd-NET Home Page/Operational/IMS Log-in*** (in accordance with DND/CF SOPs);

(4) Notify DND/CF Executives and all Level 1 organizations (in accordance with DND/CF SOPs);

(5) Executive briefing to DM, CDS and others as invited;

(6) DND/CF Level 1 representatives (Crisis Response Team) assemble in the Strategic Situation Centre;

(7) DND/CF BCP Action Team (Recovery Team – BCP specialists) work closely with the Level 1 Crisis Response Team to ensure activation of Functional (Level 1) BCPs; and

(8) Communicate with employees, partners and the public;

c. **Phase 3: Recovery.**

(1) Re-establish critical operations and services as directed by DND/CF executive authorities (DM/CDS); and

(2) Activate DND/CF recovery plans (e.g. IT/IM continuity) to ensure minimum service levels are maintained and maximum allowable downtimes are respected.

d. **Phase 4: Restoration.**

(1) Re-establish all DND/CF operations and services to normal levels.

INITIAL DM/CDS INFORMATION REQUIREMENTS

36. The initial information requirements of the DM and CDS during a disruption of service are:

a. The nature and scale of the disruption;

b. The impact the disruption will have on DND/CF operational capability and readiness; and

c. The effect on DND employees and CF members.

This information will be provided to the DM and CDS as expeditiously as possible using whatever appropriate means (e.g. briefings, telephone, and e-mail).

BCP RESPONSIBILITIES

37. The following BCP responsibilities have been assigned by Defence Administrative Orders and Directives1003-1, Business Continuity Planning Program:

a. **VCDS:**

(1) Providing leadership at the corporate level in the BCP Program as required; and

(2) Resolving conflicts of interest and priorities at the Level 1 Advisor (L1) level in respect of the BCP Program.

b. **ADM(Fin CS) and DOS (SJS):**

(1) Developing and maintaining the BCP Program to ensure the continuity of critical DND/CF services and operations and the continued availability of their associated assets, in the event of any disruption of domestic, continental or international activities;

(2) Identifying critical DND/CF services and operations and associated assets;

(3) Providing strategic direction and communication in respect of the BCP Program;

(4) Developing a comprehensive process to regularly validate and update the BCP Program;

(5) Conducting a strategic (Level 0) assessment to include:

(a) A review of DND/CF governance structures to ensure clear lines of authority, succession of command and corporate leadership, and alternate headquarters and office accommodations;

(b) The completion of a strategic Level 0 BIA to identify and prioritize critical operations and DND/CF critical services and associated assets; and

(c) The identification and review of existing DND/CF plans, measures, procedures and arrangements designed to ensure continuity of critical operations and the availability of DND/CF critical services and associated assets.

(6) Developing a comprehensive BCP to ensure the continuity of critical operations and the availability of DND/CF critical services and associated assets.

c. **Environmental Chiefs of Staff and Officers Commanding Canada COM, CEFCOM, CANSOFCOM and CANOSCOM:**

(1) Developing and maintaining critical services to support the readiness of operational maritime, land and air forces; and

(2) Directing, as appropriate, Business Continuity Planning for units and other elements under their command.

d. **ADM(IM):**

(1) Developing and maintaining:

a) Business continuity plans for the management of DND/CF critical information technology services to support managed readiness;

b) DND/ CF information technology security doctrine in support of BCP in coordination with the VCDS and DOS SJS; and

c) BCP readiness for critical national level, and distributed information systems and supporting communications.

e. **ADM(IE):**

(1) Developing and maintaining BCP for engineering standards, realty assets, environmental and nuclear safety activities, fire protection and CF family accommodation services associated with critical DND/CF operations and services.

f. **CMP and ADM(HR-Civ):**

(1) Developing and maintaining a BCP for the provision of health support services for CF members; and

(2) Developing and maintaining a BCP to ensure compensation, communication of central agency guidance and civilian administration and HR planning services for DND employees.

g. **All Level 1s:**

(1) Developing, and maintaining a BCP for critical services under their command or management; and

(2) Directing, as appropriate, Business Continuity Planning for units and other elements under their command/responsibility.

h. **DSO:**

(1) Providing general direction to the BCP Action Team on the DND/CF Security Policy as it pertains to the BCP Program; and

(2) Providing strategic advice when the BCP Action Team approaches senior managers for direction.

i. **BCP Action Team:**

(1) Making recommendations to ADM(Fin CS) and DOS SJS as required in respect of:

(a) The BCP Program policy and governance;

(b) The BIA and other templates;

(c) The commitment of financial and other resources, and the endorsement of the budget for the BCP Program; and

(d) The critical services and associated assets identified following completion of the BIA;

(2) Providing strategic direction and communication;

(3) Providing recommendations to resolve conflicts of interest and priorities;

(4) Directing training, review, testing and audit; and

(5) Directing activities to monitor overall readiness.

DND/CF BCP SUPPORTING PLANS AND PROGRAMS

38. Numerous plans and programs form an integral part of the DND/CF BCP Program. They include:

a. **Level 1 Business Continuity Plans.** The BCP Secretariat holds copies of Level 1 BCPs;

b. **DND/CF IT/IM Recovery Plan.** The DND/CF IT/IM Recovery Plan can be found at Annex B:

(1) GoC requirements for IT continuity planning are outlined in sections 12.8 and 18 of Operational Security Standard on the Management of Information Technology Security:

http://publiservice.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/23RECON_e.asp

(2) Requirements for IM continuity planning are outlined in the Policy on Information Management:

http://publiservice.tbs-sct.gc.ca/pubs_pol/ciopubs/TB_GIH/mgih-grdg_e.asp

c. **DND/CF Vital Records Plan.** All organizations within DND/CF must maintain arrangements to ensure the protection of vital records. GoC management policy requires records to be protected throughout their life cycle. Library and Archives Canada offers advice on the storage of essential records:

http://www.collectionscanada.ca/information-management/index-e.html

d. **DND/CF BCP Communication Plan.**

(1) **Internal Communications.** Keeping DND/CF employees and stakeholders informed of Departmental BCP activities is essential to ensure employees are aware of Departmental strategies, plans and procedures to deal with a disruption:

(a) Unclassified DND/CF BCP information can be found on the Defence Wide Area Network (DWAN):

http://sjs.mil.ca/sites/page-eng.asp?page=1142

(b) Classified information, such as the DND/CF Business Impact Analysis (BIA) and Threat-Risk Assessment (TRA) can be found on the secure DND network TITAN (CSNI):

TITAN (CSNI) Comd-NET Home Page/Corporate/Business Continuity Planning

(2) **External Communications.** In the event of a significant disruption, an official spokesperson for the Department will be appointed by ADM(PA); and

(3) **BCP Communications Strategy.** The detailed BCP Communications Strategy is available at Annex I.

e. **DND/CF Physical Security Plans.**

(1) DND/CF maintains extensive physical security plans. The Canadian Forces Provost Marshal (CFPM) is responsible for

developing policies and plans to guide the management of security and Military Police resources of the Department. The CFPM is responsible for all aspects of security in DND/CF. The Deputy Provost Marshal (Secur) is the Departmental Security Officer (DSO) responsible for the integration of all aspects of security in the Department of National Defence, which includes implementation of Government Security Policies and Standards, maintenance of the National Defence Security Program and development of the Canadian Forces Force Protection Program. Information on DND/CF Physical Security Instructions can be found at:

http://vcds.mil.ca/cfpm/pubs/pol-pubs/intro_e.asp

(2) GoC requirements of the Operational Security Standard on Physical Security are outlined at:

http://publiservice.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329

f. **DND/CF Emergency Management Plans.**

(1) All organizations within DND/CF maintain and regularly practice their emergency response plans. These plans have been prepared in accordance with the legal authorities that govern occupational health and safety within the GoC, namely the *Canada Labour Code* and the *Occupational Health and Safety Regulations*.

http://www.hrsdc.gc.ca/eng/labour/health_safety/index.shtml

(2) **DND/CF General Safety Programs.** Defence Administrative Order and Directive 2007-0 identifies the authorities responsible for safety in DND/CF:

http://admfincs.mil.ca/admfincs/subjects/daod/2007/0_e.asp

g. **DND/CF Pandemic Influenza Plan.** The DND/CF plan to assist in minimizing, mitigating or preventing the spread and impact of a Pandemic Influenza in order to preserve DND/CF operational capabilities and readiness, save lives, and reduce human suffering, can be found at Annex C or at:

http://sjs.mil.ca/sites/page-eng.asp?page=1416

h. **DND/CF Critical Infrastructure Protection Program.** DND/CF is working in support of Public Safety Canada to implement a National Strategy for Critical Infrastructure Protection and develop a supporting Action Plan. This collective federal/provincial/territorial and private sector approach will be used to set national priorities and requirements for critical

infrastructure protection and reduce vulnerabilities, mitigate threats, and minimize the consequences of attacks and disruptions.

i. **DND/CF Succession of Command and Alternate Headquarters Plan.**

(1) **DND Line of Authority.** Pursuant to the National Defence Act, in the temporary absence or incapacity of the MND, the Deputy Minister of National Defence may exercise all of the Minister's powers, with the exception of matters that the Minister reserves for himself or herself. The MND and DM may also appoint an ADM to act on their behalf.

(2) **CF Succession of Command and Alternate Canadian Forces Integrated Command Center (CFICC).** Defence Administrative Order and Directive 9000-1 (copy at Annex E) provides procedural guidance on the succession of command in the temporary absence or incapacity of the Chief of the Defence Staff (CDS), and the designation of an Alternate Headquarters during the inoperability of the Canadian Forces Integrated Command Center (CFICC).

DND/CF BCP READINESS

39. BCP readiness includes continuous maintenance, change management, training employees and other persons, exercising, preparing lessons learned reports and updating plans when there is a change in personnel, process, technology or departmental structure. The DND/CF BCP will be updated on an iterative basis to enable the Department to anticipate new risks and develop measures to address these risks.

a. **BCP Document Revision Control.** Given the "evergreen" nature of the BCP Program (BCPP), there will be constant updating of BCPP documentation. This will necessitate a process to ensure that the most current and accurate versions of all documentation are in use at all times, and that the same versions are available to all stakeholders. The BCPP Document Revision Control operating concept includes the following:

(1) BCPP documentation includes, but is not limited to:

- Relevant DAODs;
- Threat and Risk Assessments (TRA);
- Business Impact Analyses (BIA);
- Business Continuity Plans (BCP); and
- Pandemic Plans.

(2) BCPP documentation should be revised every time there is a change to the organization that has an impact on the BCP program. This includes, but is not limited to:

- Organizational changes;
- Changes to mandate or function;
- New accommodation;
- Significant changes to existing accommodation;
- New IM/IT or communications equipment;
- Significant changes to existing IM/IT or communication equipment; and
- Personnel changes requiring amendments to contact lists.

(3) L0 will refresh its BCP annually or more often as required;

(4) L1 organizations will refresh their BCPs annually or more often as required;

(5) Current copies of all L0 and L1 BCPP documentation shall be held in a Central BCPP Repository by the BCPP Secretariat; and

(6) Copies of all changes to any L0 and L1 BCPP documentation shall be submitted to the Central BCPP Repository.

b. **Central BCPP Repository.** The BCP Secretariat has established a Central BCPP Repository which holds copies of all current L0 and L1 BCP documentation in a secure location in both hard and electronic formats;

c. **BCPP Documentation Updates.** Whenever BCP documentation is updated, either due to the annual refreshing or other changes necessitating amendments, the amended document with the annotated changes shall be submitted to the BCP Secretariat within 30 days of publication.

d. **BCP Exercises.** Testing and validating the BCPs will be done on a regular basis, with a Level 0 exercise conducted at a minimum every two years. Please see the DND/CF Exercise Strategy at Annex J.

e. **BCP Training Opportunities and Courses.** The Canada School of Public Service conducts a course specifically on BCP. Information is available at:

http://www.csps-efpc.gc.ca/cat/det-eng.asp?courseno=T726

LIST OF ANNEXES