National Defence / Défense nationale

Department of National Defence
Canadian Forces

BUSINESS CONTINUITY PLAN

"Ensuring Defence Mission Success in Times of Crisis"

DRAFT
Version 2b
13 March 09

UNCLASSIFIED

Canada

This page intentionally left blank.

Table of Contents

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

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 Government Security Policy (GSP), 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 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 any event, and to recover and restore DND/CF operations and services to minimum levels following a traumatic event, emergency or disruption.

AUTHORITY

4. The 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.

APPLICABILITY

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

KEY DEFINITIONS AND REFERENCES

6. A complete list of key references and glossary of BCP terms can be found at annexes G and H 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 critical services and associated assets;

b. **Critical Operations and Services** are Departmental 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 Minimum Service Levels (MSL) for critical operations and services; and

c. **Business Impact Analysis (BIA)** is the process of analyzing the degree to which a Department is exposed to risks, and impacts that could effect 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 Program, while Public Safety Canada is responsible for ensuring and validating that departments are complying with the GSP.

NATIONAL POLICY OBJECTIVES

8. In accordance with the GSP, the continued delivery of government services must be assured. The GoC BCP Program is designed to protect the resources on which the government relies. The objective of the GoC BCP Program 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 BCP Program 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 and 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 business continuity plans;
- 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 complete 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 – Key References).

METHODOLOGY

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

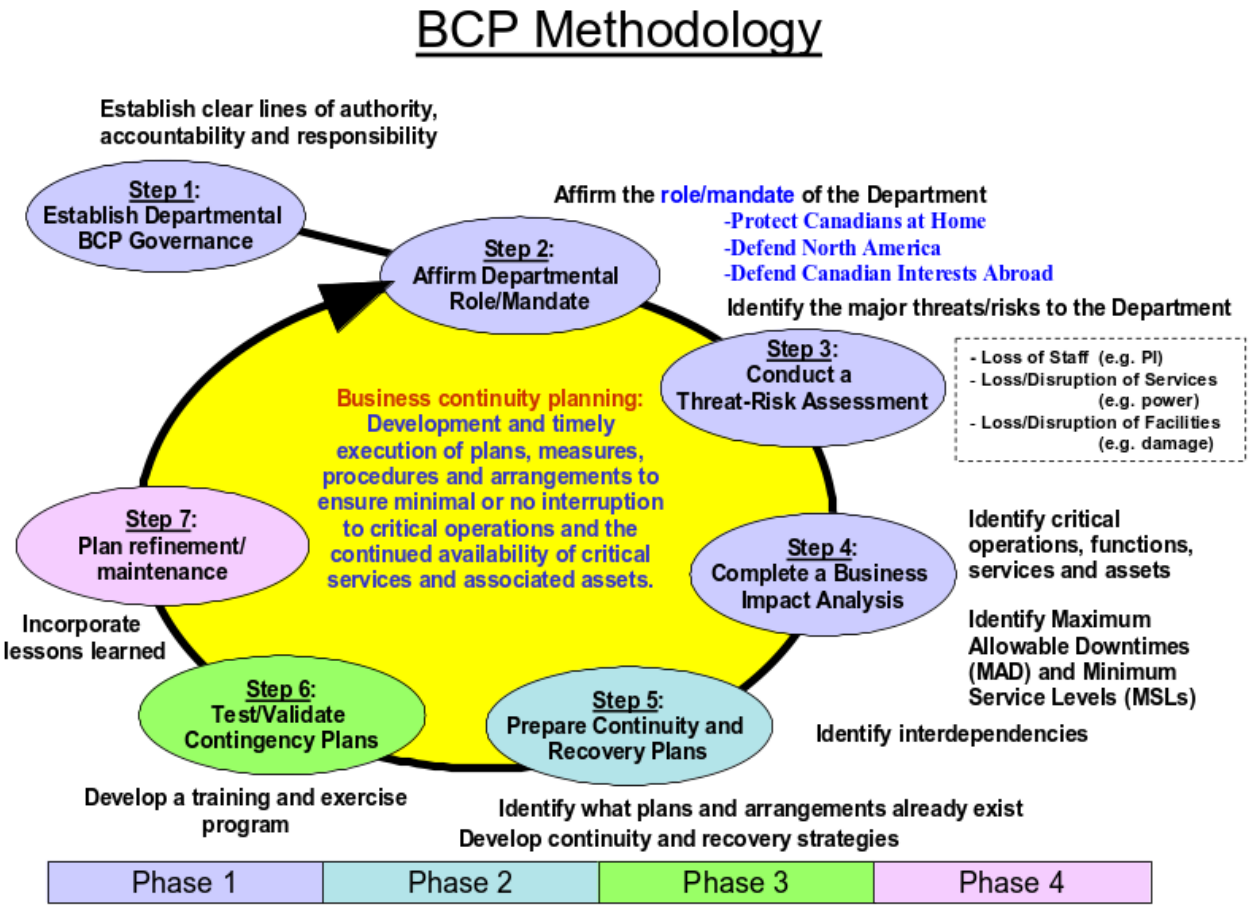

Figure 1 – DND/CF BCP Methodology

ROLE AND MANDATE OF DND/CF

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

a. **Protect Canadians at Home** – *protecting Canadians and defending Canadian sovereignty;*

b. **Defend North America** – *working with Canada's closest ally, the United States, to defend North America*; and

c. **Defend Canadian Interests Abroad** – *operations around the world*.

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 the largest federal department in Canada, with over 25,000 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, numbering approximately:

a. 62,000 Regular Force members; and

b. 25,000 Reserve Force members, including 4,000 Canadian Rangers.

19. **DND 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 BCP is included as Annex E to this document.

b. **Communications Security Establishment (CSE).** CSE is a cryptologic agency that collects 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. CSE has a separate BCP (please see link at Annex F).

c. **Office of the Commissioner of CSE.** The commissioner of CSE, appointed by the Governor in Council, is responsible for reviewing the activities of the Establishment 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 Establishment that the Commissioner believes may not be in compliance with the law. The office of the Commissioner of CSE has a separate BCP (please see link at Annex F)

e. **Military Police Complaints Commission (MPCC).** MPCC is responsible for examining any 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 (please see link at Annex F).

f. **Canadian Forces Grievance Board (CFGB).** CFGB is an impartial, independent body responsible for reviewing the grievances submitted to it military members and communicating its conclusions and recommendations to the CDS. CFGB has a separate BCP (please see link at Annex F).

g. **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 (please see link at Annex F).

20. **Defence Management System.** Management of Canada's Defence Programme, 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 (L1)[1] business plans for the implementation of the Defence Services Program. The table at Figure 2 provides an overview of DND/CF Level 0 and Level 1 organizational elements, and the high level organization is depicted in the chart at Figure 3. 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 G – Key References).

[1] 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 CDS	Vice Chief of the Defence Staff
	Assistant Deputy Minister (Information Management)
	Assistant Deputy Minister (Science and Technology)
	Chief of Review Services
	DND/CF Legal Advisor *(also responsible to the DM of the dept of Justice)*
	Assistant Deputy Minister (Public Affairs)
	Chief of Defence Intelligence *(under authority of the VCDS)*
Level 1s 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	Canadian Security Establishment (CSE)
	National Search and Rescue (SAR) Secretariat
	Ombudsman
	Military Police Complaints Commission
	Chief Military Judge
	Judge Advocate General
	CF Grievance Board

= *civilian incumbent* = *military incumbent*

Figure 2 - DND Organizational Elements

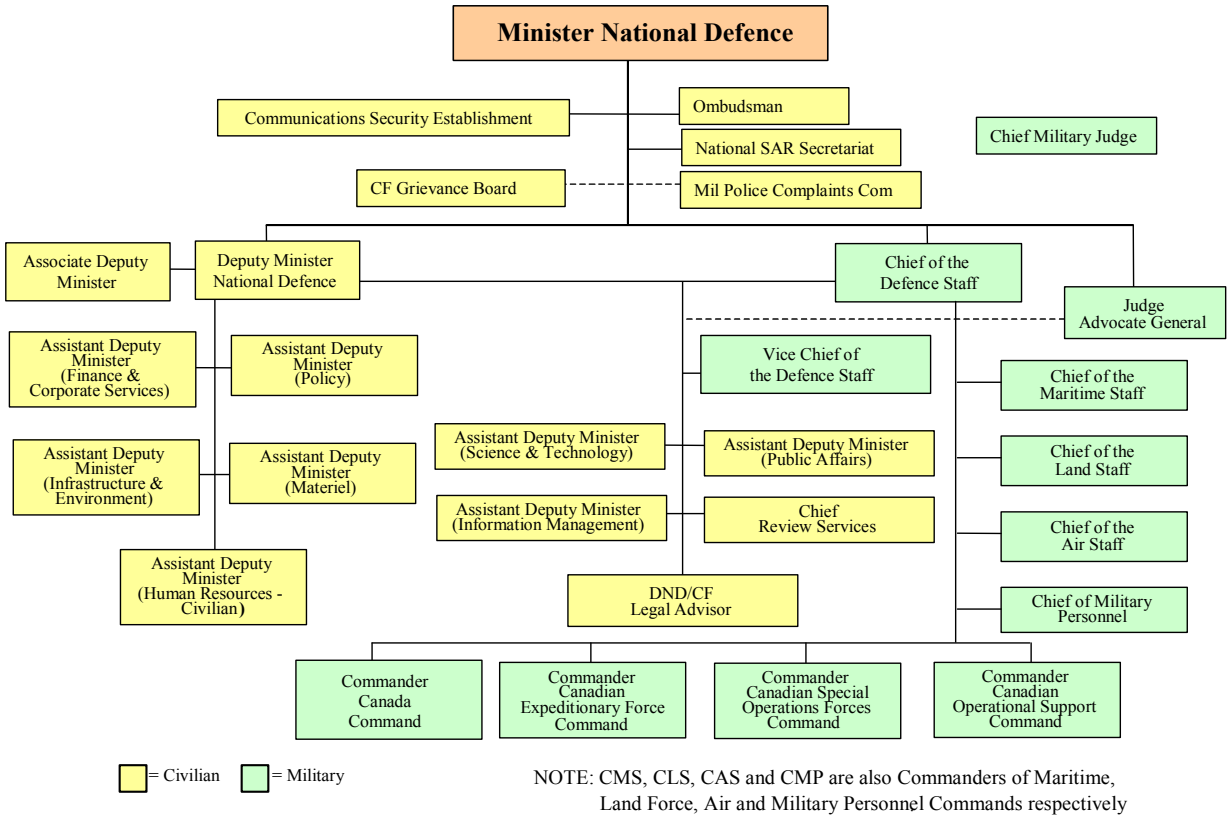

Figure 3 – DND Organization

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 Defence Management Oversight Committee (DMOC), 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 organizations within DND/CF, as well as key representatives such as the Departmental Security Officer (DSO), are members of the DND/CF BCP Action Team (Director level); and

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

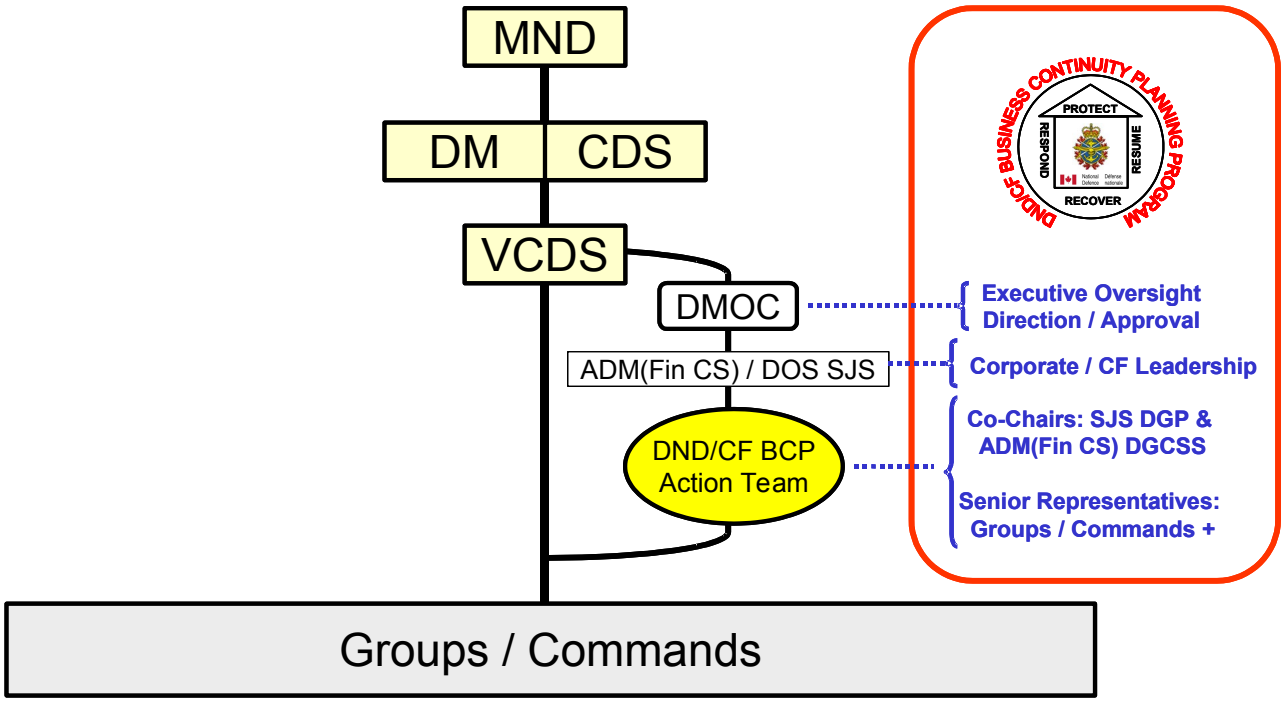

Figure 4 – DND/CF BCP Governance

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 operations and services. These events can be categorized as resulting in:

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

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

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

24. The complete DND/CF Threat and Risk Assessment is classified SECRET. It can be found on the secure DND/CF network, under TITAN/Corporate View/Business Continuity Planning.

BUSINESS IMPACT ANALYSIS (BIA)

25. **DND/CF Critical Operations and Services.** 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	
Protect Canadians at Home (Defence of 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
Defence of North America	Aerospace Warning and Control (NORAD Agreement)
	Maritime Warning (NORAD Agreement)
Defend Canadian Interests Abroad (Contributing to International Peace and Security)	Evacuation of Canadians from Threatened Areas
	Expeditionary Operations
Continuity of 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 operation or services is classified SECRET. It can be found on the secure DND/CF network, under TITAN/Corporate View/Business Continuity Planning.

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

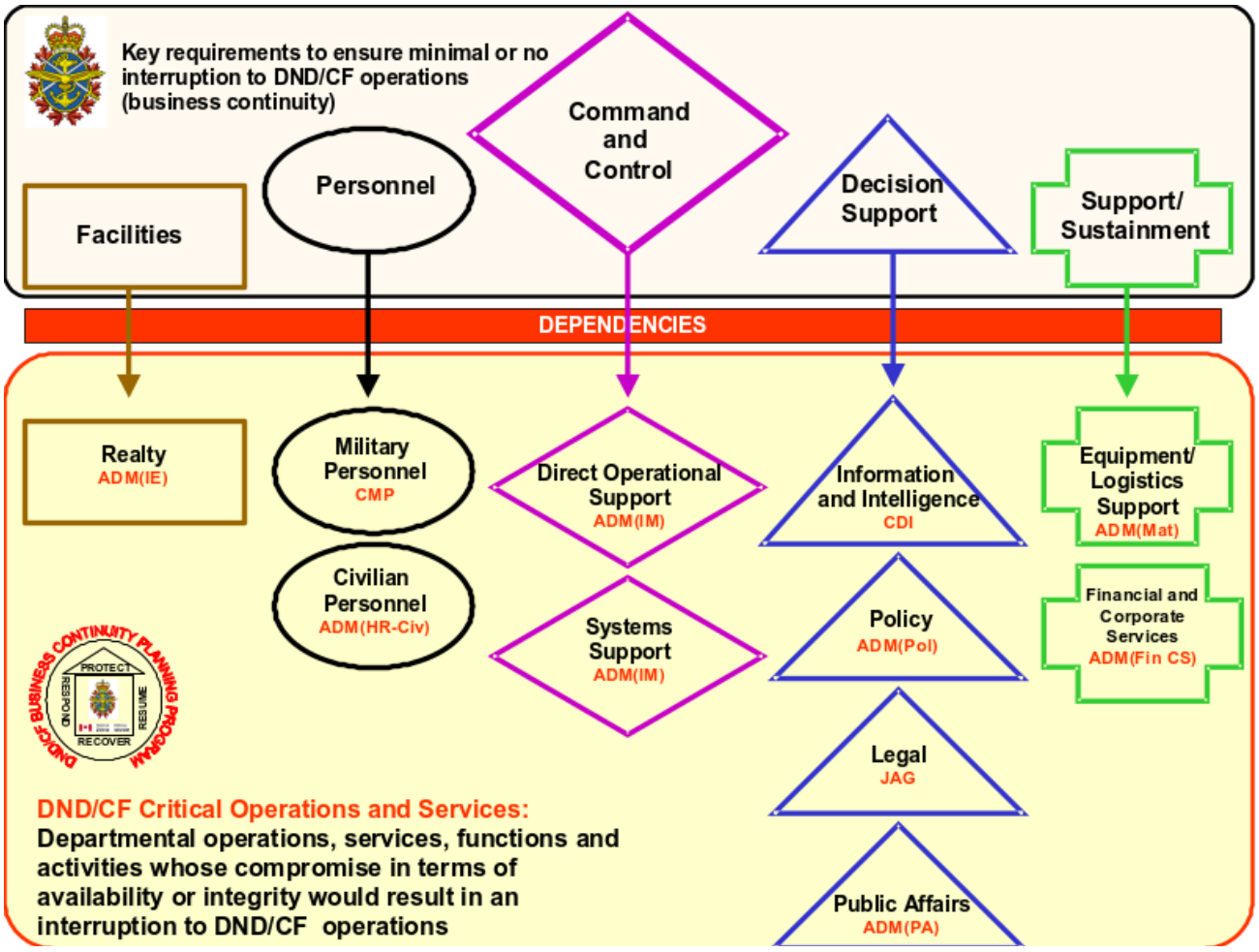

Figure 6 – Key Requirements to Ensure Minimal or No Interruption to DND/CF Operations

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 Chief of Defence Intelligence (CDI) 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 operations and services;

b. The duration of the disruption will be a maximum of 30 days;

c. Key personnel will be unavailable; and

d. The alternate national DND/CF NDCC site 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 form 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 operational capacity.

CONCEPT OF OPERATIONS

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

a. Facilities.

(1) An alternate site (national headquarters) 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 services (sources of electricity, 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;

(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

(6) DND/CF will create a BCP human resource strategy (following guidance from TBS).

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 (de-centralization 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 DND/CF recovery and response plans are to be developed for:

(a) IT/IM continuity;

(b) Communications; and

(c) 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.

f. **Sustainment.**

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

(2) 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 (National Defence Command Center);

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

(3) Details of incidents/events are populated on the DND/CF Incident Management System located on the CNSI, URL: http://ims.cmil.ca (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 National Defence Command 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.**

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 means (e.g. briefings, telephone, e-mail) are appropriate.

BCP RESPONSIBILITIES

37. The following BCP responsibilities have been assigned by Defence Administrative Orders and Directive1003-1, 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. **DOS (SJS) and ADM(Fin CS).**

(1) developing and maintaining the BCP Program to ensure 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;

(2) identifying critical operations, and DND and CF critical services and associated assets;

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

(4) developing a comprehensive program to regularly validate and update the BCP Program;

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

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

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

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

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

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

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

(2) conducting, as appropriate, BRP for units and other elements under their command.

d. **ADM(IM).**

Developing and maintaining:

(1) business continuity plans for the management of DND and CF critical information technology services to support managed readiness;

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

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

e. **ADM(IE).**

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

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

(1) Developing and maintaining BCP for CF members to provide health support services

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

g. **All Level 1s.**

(1) Developing, and maintaining business continuity plans for critical services under their command or management; and

(2) conducting, as appropriate, BRP for units and other elements under their command.

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 the 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) identified critical services and associated assets after 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. They include:

a. **Level 1 Business Continuity Plans.** Links to Level 1 BCPs can be found at Annex A.

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

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

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

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

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 maintain arrangements to ensure vital records protection. 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):

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).

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

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. 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, 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/org/intro_e.asp

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

http://publiservice.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/CHAPT2-4_e.asp

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.hr-rh/osh-sst/index-eng.asp

(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 PI in order to preserve DND/CF operational capabilities and readiness, save lives, and reduce human suffering can be found at Annnex C or:

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 Headquarters.** Defence Administrative Order and Directive 9000-1 (copy at Annex D) 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 National Defence Headquarters (NDHQ) /National Defence Command Centre (NDCC). Please see the VCDS BCP at Annex A for details.

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 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 no 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 BCPP. This includes, but is no 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.

(4) L1 organizations will refresh their BCPs annually.

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

(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 BCPP Secretariat has established a Central BCPP Repository which holds copies of all current L0 and L1 and BCPP 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 BCPP 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 A, Appendix 6.

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/corporate/list_e.asp?value=all&lang=E&loid=326

ANNEXES

ANNEX A – DND/CF Response Plan

Appendix 1 – DND/CF Senior Leadership Contact List
Appendix 2 – BCP Action Team Contact List
Appendix 3 – DND/CF BCP Action Checklist
Appendix 4 – DND/CF BCP Decision Chart
Appendix 5 – DND/CF BCP Communications Strategy
Appendix 6 – DND/CF BCP Exercise Strategy
Sub-Appendix 6-1 – DND/CF Exercise Scenarios
Appendix 7 – Level 1 Business Continuity Plans

ANNEX B – DND/CF IM/IT Recovery Plan

ANNEX C – DND/CF Pandemic Influenza Plan

Appendix 1 – DND/CF Pandemic Influenza Plan
Appendix 2 – CDS Supplementary Directive – Pandemic Influenza

ANNEX D – CF Succession of Command and Alternate Headquarters Plan

Appendix 1 – BCP Accommodations

ANNEX E – National Search and Rescue Secretariat BCP

ANNEX F – Portfolio Organizations BCPs

ANNEX G – Key References

ANNEX H – Glossary