National Defence / Défense nationale

DND/CF
BUSINESS CONTINUITY PLAN

ANNEX B

DND/CF IM/IT RECOVERY PLAN

January 2010

DND/CF BCP SECRETARIAT
SJS - DGCSS

DND/CF IM/IT RECOVERY PLAN

References: A. 3120-1 (SJS CANUS Plans) DM/CDS Initiating Directive – DND/CF Continuity of Critical Operations and Services (Business Continuity Plan) 5 January 2007 (http://sjs.mil.ca/sites/page-eng.asp?page=1142)
B. Communications Policy of the Government of Canada August 1, 2006 (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12316)
C. TBS Public Service Readiness Plan 2008
C. TB Operational Security Standard - Business Continuity Planning (BCP) Program (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12324)
E. Operational Security Standard: Management of Information Technology Security (MITS) (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328)
F. DAOD 1003-0 Business Continuity Planning (http://admfincs.mil.ca/admfincs/subjects/daod/1003/0_e.asp)
G. DAOD 1003-BCPP Business Continuity Planning Program (http://admfincs.mil.ca/admfincs/subjects/daod/1003/1_e.asp)

INTRODUCTION

Background

1. Information systems are vulnerable to a variety of disruptions, ranging from mild (e.g., short-term power outage, disk drive failure) to severe (e.g., equipment destruction, fire). Much vulnerability may be minimized or eliminated through technical, management, or operational solutions as part of the organization's Risk Management effort; however, it is virtually impossible to completely eliminate all risks[1]. Contingency Planning is designed to mitigate the risk of system and service unavailability by focusing effective and efficient recovery solutions.

2. This Annex discusses the ways in which IT (Information Technology) Contingency Planning fits into an organization's larger Risk Management, Security, and Emergency Preparedness programs. The Concept of Operations (CONOP) portion of the document identifies those information systems deemed as supporting CF/DND critical services and operations. The CONOP provides a prioritization scheme for recovery of such information systems to ensure those supporting the most critical aspects of the organization's operations are identified to be undertaken ahead of lower priority systems for recovery efforts in the event of multiple, simultaneous disruptions. In virtually all cases, information system disruptions affecting many users will be prioritized ahead of disruptions affecting a single or very few users.

[1] For example, in many cases, critical resources may reside outside the organization's control (such as electric power or telecommunications), and the organization may be unable to ensure their availability.

Contingency Planning and Risk Management

3. Risk Management encompasses a broad range of activities to identify, control, and mitigate risks to an IT system. Risk Management activities from the IT Contingency Planning perspective have two primary functions. First, Risk Management should identify threats and vulnerabilities so that appropriate controls can be put into place to either prevent incidents from happening or to limit the effects of an incident. These security controls protect an IT system against three classifications of threats:

a. Natural - e.g., hurricane, tornado, flood, and fire;
b. Human - e.g., operator error, sabotage, implant of malicious code, and terrorist attacks; and
c. Technical Environment - e.g., equipment failure, software error, telecommunications network outage, and electric power failure.

4. Second, Risk Management should identify residual risks for which contingency plans must be put into place. The contingency plan, therefore, is very closely tied to the results of the risk assessment and its mitigation process. Figure 1 illustrates the relationship between identifying and implementing security controls, developing and maintaining the contingency plan, and implementing the contingency plan once the event has occurred.

Figure 1 - Contingency Planning as an Element of Risk Management Implementation

5. To effectively determine the specific risks to an IT system during service interruption, a risk assessment of the IT system technical environment is required. A thorough risk assessment should identify the system vulnerabilities, threat, and current controls and attempt to determine the risk based on the likelihood and threat impact. These risks should then be assessed and a risk level assigned.

6. Because risks can vary over time and new risks may replace old ones as a system evolves, the Risk Management process must be ongoing and dynamic (reactive to changes in the technical environment) and the threat risk assessment updated frequently to ensure its currency. The staff responsible for IT Contingency Planning must be aware of risks to the system and recognize whether the current contingency plan is able to address residual risks completely and effectively. The shifting risk spectrum necessitates ongoing contingency plan maintenance and testing, in addition to periodic reviews.

IT Preventive Controls

7. Where feasible and cost-effective, preventive methods are preferable to actions that may be necessary to recover the system after a disruption. A wide variety of preventive controls are available, depending on system type and configuration; however, some common measures are listed below:

a. Regular preventive maintenance;
b. Appropriately sized uninterruptible power supplies (UPS) to provide short-term backup power to all system components (including environmental and safety controls);
c. Gasoline or diesel powered generators to provide long-term backup power;
d. Air-conditioning systems with adequate excess capacity to permit failure of certain components, such as a compressor;
e. Fire suppression systems;
f. Fire and smoke detectors;
g. Water sensors in the computer room ceiling and floor;
h. Plastic tarps that may be unrolled over IT equipment to protect it from water damage;
i. Heat-resistant and waterproof containers for backup media and vital non-electronic records;
j. Emergency master system shutdown switch;
k. Offsite storage of backup media, non-electronic records, and system documentation;
l. Technical security controls, such as cryptographic key management and least-privilege access controls; and
m. Frequent, scheduled backups.

8. Preventive controls should be documented in the contingency plan, and personnel associated with the system should be trained on how and when to use the controls. These controls should be maintained in good condition to ensure their effectiveness in an emergency.

IT Contingency Planning

9. IT Contingency Planning represents a broad scope of activities designed to sustain and recover critical IT services following an emergency. IT Contingency Planning fits into a much broader emergency preparedness environment that includes organizational and business process continuity and disaster recovery planning. Ultimately, an organization would use a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the organization's IT systems, business processes, and the facility. The inherent relationship between an IT system and the business process it supports, requires coordination between each plan during development and updates to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts. Since an IT contingency plan should be

developed for each major application and general support system, multiple contingency plans may be maintained within the organization's Business Continuity Plan (BCP).

10. As the IT contingency policy and program are developed, they should be coordinated with related agency activities, including IT security, physical security, human resources, IT operations, and emergency preparedness functions. IT contingency activities should be compatible with program requirements for these areas, and contingency personnel should coordinate with representatives from each area to remain aware of new or evolving policies, programs, or capabilities. Contingency plans must be written in coordination with other existing plans associated with systems. Such plans include the following:

a. Security-related plans, such as system security plans;
b. Facility-level plans, such as the emergency evacuation procedures; and
c. Organization-level plans, such as business resumption and critical infrastructure protection (CIP) plans.

Purpose

11. Information Technology (IT) and Information Management (IM) systems are vital elements in DND/CF processes. IT resources are so essential to the organization's success; it is critical that the services provided by these systems are able to operate effectively without excessive interruption. Contingency Planning supports this requirement by establishing thorough plans and procedures and technical measures that can enable a system to be recovered quickly and effectively following a service disruption or disaster.

12. IT Contingency Planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of IT systems, operations, and data after a disruption. Contingency Planning generally includes one or more of the approaches to restore disrupted IT services:

a. Restoring IT operations at an alternate location;
b. Recovering IT operations using alternate equipment; and
c. Performing some or all of the affected business processes using non-IT (i.e. manual) means (typically acceptable for only short-term disruptions).

Applicability

13. This Annex helps provide guidance to individuals responsible for preparing and maintaining BCPs at various levels of the organization. The DND/CF Business Continuity Plan identifies what have been recognized as essential information systems and recommends applicable MADs (Maximum Allowable Downtimes) for each so that organizations can make contingency plans to use alternate means to continue delivery of critical services throughout the probable duration of loss of information services.

14. The Annex is to be used both by L1 BCP Coords to adjust their organizations' expectations of information systems availability, as well as by information systems service providers to assist in selecting and achieving appropriate MADs for their organization. The MAD levels outlined and ability to restore systems is based on "current capability" within DND/CF and the Information Management Group, and not necessarily what other Level 1 planners desire. The intent of the BCP is to reflect current capability and restoral abilities should an emergency occur in the present, not the capability that is foreseen in the future. Level 1 planners must develop alternative "work around" solutions to adapt for prolonged outages that may occur in select areas to cover the gap between downtime and restoral and enable the eventual return to normal operations upon termination of the crisis.

Assumptions

15. It must be understood that information systems within DND/CF have extremely complex interdependencies including electrical power, commercial bandwidth, multiple devices such as routers, modems and servers and building internal wiring. It is therefore extremely difficult to quantify maximum allowable downtimes (MAD) for such systems that would take into account all such dependencies. The assumption associated with each MAD provided for a specific information system should be that the failure occurs solely within that system or equipment identified and that it is not caused by an underlying interdependency.

16. Information system service providers have become extremely adept at detecting the point of failure in such a system, however some failures are difficult to diagnose, particularly when multiple interdependent systems experience failures concurrently. Such unusual circumstances could cause an outage of duration well beyond the MAD identified for a specific information system. Organizational BCPs should therefore take into account the potential for loss of access to a particular information system for a duration exceeding the MAD.

CONCEPT OF OPERATIONS

17. Many contingency measures can be taken by information system support organizations to improve system resiliency in the event of a disruptive incident. Several of these are common to all IT systems. Common considerations assumed in use within the DND/CF information systems include:

a. Alternate or duplicate sites and/or servers and key network elements;
b. Frequency of backup and offsite storage of data, applications, and the operating system;
c. Redundancy of critical system components or capabilities;
d. Documentation of system configurations and requirements;
e. Interoperability between system components and between primary and alternate site equipment to expedite system recovery; and

f. Appropriately sized and configured power management systems and environmental controls.

18. The critical information systems within DND/CF have been divided into three categories, as follows:

a. Category A - Operational/Command Systems (Classified)
b. Category B - Corporate/Enterprise Systems (Designated)
c. Category C - Administrative and Telecommunications

19. Within each category, there are varying priority levels of information systems. Across DND/CF in general - all other factors being equal - the identification of an information system as an operational system would normally imply that it is more important or at higher priority for restoral than a corporate/enterprise or an administrative system as it is implied to exist to support command and control of the CF.

20. Information systems have been assigned Operational, Technical and Security Authorities (OA, TA and SA).[2] Priorities for information systems are given as general guidance at this point, based on a combination of assessments from information system service provider staff (Technical Authority) and system availability requirements identified by various Level One user communities. Actual priority decisions under the circumstances of a disruptive event will always be a function of command (Operational Authority) based on an appreciation of the variables at play at a given time. Setting network restoration priorities is a primary responsibility of a network's Operational Authority.

21. The Security Authority (SA) is the office that has the authority to set CIS security standards, develop and recommend network security policies for endorsement by the OA and TA and approval by the Departmental SA.[3] The Departmental SA is also referred to as the Departmental IT Security Coordinator and is accountable to the Departmental Security Officer for managing the departmental information technology security program. The ITS Coordinator shall, among other duties, coordinate disaster recovery plans with business continuity plans.[4] The Chief Information Officer, Departmental Security Officer, IT Security Coordinator and the Business Continuity Planning Coordinator must work together to ensure a comprehensive approach to continuous service delivery.[5]

---

[2] Definitions of these terms are provided in the VCDS Direction on CF Integrated Command and Control Information Systems dated 18 September 2006 available through the DND Intranet at: http://cfd.mil.ca/sites/page-eng.asp?page=1101

[3] Definitions of these terms are provided in the VCDS Direction on CF Integrated Command and Control Information Systems dated 18 September 2006 available through the DND Intranet at: http://cfd.mil.ca/sites/page-eng.asp?page=1101

[4] Defence Security Manual - Information Technology Security Policy, Annex C, available through the DND Intranet at: http://img.mil.ca/natsvcs/imit_security/itsec_polstnds/docs/dsm_part7_chp1_e.pdf

[5] TBS Operational Security Standard: Management of Information Technology Security (MITS) available online at: http://publiservice.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328&section=text#sec2.3

22. The continuously increasing and dynamic nature of IT security threats could result in significant disruption to IM and IT services. The standard for management of IT security requires that departments have in place processes to detect, respond to and recover from IT security incidents. [6]

23. From a horizontal perspective, the standard of management of IT security also requires departments to take into account the impact of incidents on other federal organizations and to report IT security incidents to Public Safety Canada. As part of the Government Operations Centre, Public Safety Canada operates the Canadian Cyber Incident Response Centre (CCIRC). The CCIRC is responsible for monitoring threats, issuing alerts and advisories and coordinating the response to cyber security incidents.

24. To detect incidents, technical and security authorities can, subject to applicable laws and relevant policies, use firewalls and routers, audit logs, virus and malicious code detection software, system performance tools, health-monitoring tools, integrity checkers, and host- and network-based intrusion detection systems. The rigor and extent of detection will depend on the level of risk, including the sensitivity (in terms of confidentiality, availability and integrity) and the system exposure.

25. To protect information and ensure service delivery, authorities must continuously monitor system performance to rapidly detect:

a. Attempts (failed or successful) to gain unauthorized access to a system, or to bypass security mechanisms;
b. Unauthorized probes or scans to identify system vulnerabilities;
c. Unplanned disruption of systems or services;
d. Denial-of-service attacks;
e. Unauthorized changes to system hardware, firmware, or software;
f. System performance anomalies; and
g. Known attack signatures.

26. At a minimum, technical authorities must include a security audit log function in all IT systems. They must incorporate automated, real-time, incident detection tools in high risk systems.[7] Access to firewall logs also is often key to helping identify intrusions into information systems.

27. Within DND/CF CFNOC (the Canadian Forces Network Operations Centre) is the focal point for Information Technology Infrastructure (ITI) activity. CFNOC operates and manages the national systems, performing the network protection role through the Computer Network Defence Troop (CND Tp). The mission of the CND Tp is to conduct proactive defensive network security operations to ensure the confidentiality, integrity and availability of DND/CF networks in all information domains.

---

[6] The Public Service Readiness Plan, TBS 2008, page 93.
[7] TBS Operational Security Standard: Management of Information Technology Security (MITS) available online at:
http://publiservice.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328&section=text#sec2.3

28. The CND Tp Responsibilities include:

a. Information System Security Incident Management;
b. Operating and Monitoring Network Sensors;
c. Patch and Vulnerability Management; and
d. User Information Security Awareness.[8]

29. The following sections detail various types of priority information systems identified across DND/CF as essential to continuity of critical operations and to assuring the availability of critical services and assets. Under normal circumstances and with all else being equal, multiple information system disruptions will normally result in the disruptions affecting the widest number of users being addressed ahead of those affecting smaller numbers or single users.

30. The Maximum Allowable Downtime for each critical service was determined based on the following definition provided within the DND/CF BCP:

a. Maximum Allowable Downtime (MAD): The MAD is the longest period of time for which a service can be unavailable or degraded before a high degree of injury results; and
b. Minimum Service Level (MSL): The MSL is the level of service delivery that is essential to avoid a high degree of injury. It is the minimum level that must be maintained until full recovery is achieved.

31. Based on the fact that a majority of IT systems/services do not function independently, but have dependencies on other systems/services to support Business Processes, it should be taken into consideration that realistic MADs must consider these services/systems dependencies and interdependencies. Based on these definitions it should be noted that from a L1 perspective, the MAD for each critical service should also be re-evaluated with respect to dependency and interdependency of related services amongst the L2 organizations within ADM (IM) as well, in order to arrive at more precise MADs. It is understood that this activity will eventually be coordinated by the ADM (IM) Level 1 BCP Coordination Office.

TELEPHONY

32. Disruptive events have the potential to interfere with many elements of the information systems of the organization. While it may take some time to determine the level of disruption within data systems, it is usually quite straightforward to determine whether or not telephone systems have suffered disruptions. Culturally, individuals tend to rely on the telephone system as the first means of communication in the event of a crisis. The DND/CF telephony infrastructure is provided via means of leased services from the commercial service providers in this area (i.e. Bell Canada, Telus, etc.)

[8] Description of Incident Handling and Vulnerability Assessment (CND Tp) available on the DND Intranet at http://img.mil.ca/natsvcs/imit_security/network/index_e.asp

33. Much of the emphasis on managing the organization's reaction to a disruptive event is focused on communicating to and among the relevant crisis response team. The most common element to the planning for such communications across the organization has been found to be call-out telephone lists. For these reasons, telephony responsiveness is accorded a very high priority in the list of systems requiring restoral activities should they be disrupted for some reason.

34. In some cases, (ie. The Canadian Defence Red Switch Network - CDRSN) the same OA / TA / SA construct exists as for networks; therefore restoral priorities are part of the designated OA's responsibilities.

35. The list of telephony systems and recommended MADs is displayed in the table following:

Priority for Restoral	**Category of System**	**Information System**	**Maximum Allowable Downtime (MAD)**
1	A	Defence Red Switch Network/Canadian Defence Red Switch Network (DRSN/CDRSN)	24-48 hrs
2	C	Commercial Telephones (landline)	2 hrs
3	C	Canadian Switched Network (CSN)/Defense Switched Network	2 hrs
4	A	Secure Telephone Equipment (STE)	2 hrs
5	A	Sectera secure cell phone	2 hrs
6	A	Iridium Satellite Telephones	2 hrs
7	A	Commercial Pagers	2 hrs
8	A	Mandrake Voice over IP (VOIP) telephone (Govt of Canada)	4 hrs
9	B	Video Conferencing Network(s) Bridging Centres Bridge/Switch Repair or Replacement	1-6 hrs 48 – 72 hrs
10	B	Secure Video Conferencing Network (SVCN) SVTC Terminal Eqpt Investigation and Repair	24 hrs 1-4 days (dependent on location)
11	B	Defence Video Conferencing Network (DVCN – unclassified) DVTC Terminal Eqpt Investigation	24 hrs 1-4 days

		and Repair	(dependent on location)
12	C	Initial Voice Switched Network (IVSN)	24 hrs
13	C	Commercial cell phone service	24 hrs
14	C	Secure Fax	24 hrs
15	C	Unclassified Fax	24 hrs

WIDE AREA NETWORKS (WANs) – CLASSIFIED SYSTEMS

36. A wide area network (WAN) is a data communications network that consists of two or more LANs that are dispersed over a wide geographical area. Communications links, usually provided by a public carrier, enable one LAN to interact with other LANs.

37. Within DND/CF there are many wide area networks, frequently existing for very specialized functions, so many that it is nearly impossible to denote them all. The Classified WANs in particular typically form part of multinational or multi-agency information system and could potentially suffer losses of service or connectivity entirely out of control of the internal service support organization. Networks usually have designated OA, TA and SA to assess risks and assign restoral priorities. The emphasis for priority of restoral on networks within DND/CF generally focuses on the classified networks, to ensure continuity of command and control of CF operations. The following table recommends the restoral priorities for some of the classified wide area networks within DND/CF:

Priority for Restoral	**Category of System**	**Information System**	**Maximum Allowable Downtime (MAD)**
1	A	Consolidated Secret Network Infrastructure (CSNI) e-mail capability	1 hr
2	A	CSNI Instant Persistent War Room Portal (IPWAR)	1 hr
3	A	Secret Internet Protocol Router Network (SIPRNet) RELCAN COP	1 hr
4	A	Joint Staff Information System	1 hr
5	A	SPARTAN	2 hrs
6	A	CHINOOK	2 hrs
7	A	STONEGHOST (e-mail and web access)	2 hrs
8	A	Portable SIGINT Support System (PSSS)	2 hrs
9	A	National Counter Intelligence Unit	4 hrs

		(NCIU) WAN	
10	A	Enhanced Imagery Reporting and Exploitation System	4 hrs
11	A	Automated Defence Data Network (ADDN)/ Common Military Messaging System (CMMS)	4 hrs
12	A	Canadian Portal for Imagery and Geospatial Services (CPIGS)	4 hrs
13	A	Global Command and Control System – Maritime (GCCS – M)	4 hrs
14	A	Land Force Command and Control Info System (LCCIS)	4 hrs
15	A	Air Force Command and Control Info System (AFCCIS)	4 hrs
16	A	Combined Enterprise Regional Information Exchange System (CENTRIXS)	4 hrs
17	A	Consolidated Secret Network Infrastructure (CSNI) Incident Management System (IMS)	24 hrs
18	A	Secure Integrated Network (SIGNET) – DFAIT system	24 hrs
19	A	Battlefield Intelligence Collection and Exploitation System (BICES) – NATO system	24 hrs
20	A	Logistic Functional Area Services (LOGFAS)	24 hrs
21	A	Consolidated Secret Network Infrastructure (CSNI) backbone	24 hrs
22	A	Root DNS server for cmil.ca	48 hrs

38. MADs identified for classified applications are valid assuming that the bearer system, the CSNI backbone, is functional. Given that CSNI backbone outages are likely to involve much greater complexity, and a confirmed reliance on outside service providers, the MAD for the CSNI backbone may be much greater than for restoral of a single application. In fact, in many cases applications are replicated on hot standby servers, which can greatly facilitate their restoral and reduce the MAD. Thus the reason that the MAD for an application in many cases is significantly less than the MAD for the backbone on which it is dependent.

WIDE AREA NETWORKS (WANs) – UNCLASSIFIED SYSTEMS – AND WEB SITES

39. The most commonly used unclassified WAN across DND/CF is the DWAN, which provides Microsoft Office capabilities (through centralized servers), enterprise applications and external websites as well as the internal web-based Defence Information Network (DIN). The DWAN was originally developed by ADM(IM) as an administrative network and resourced accordingly. The backbone for the system was created in the most cost-effective method possible. Significant risks of outages exist and are created by single points of failure across the system. ADM(IM) is acknowledged as the DWAN's OA and TA and has identified a recovery time objective (RTO) for the overall network of 7 days. Organizational BCPs should provide contingency plans for potential loss of the DWAN for up to a week.

40. A Web site is used for information dissemination on the Internet or an intranet. The Web site is created in Hypertext Markup Language (HTML) code that may be read by a Web browser on a client machine. A Web site is hosted on a computer (Web server) that serves Web pages to the requesting client browser. The Web server hosts the components of a Web site (e.g., pages, scripts, programs, and multimedia files) and serves them using the Hypertext Transfer Protocol (HTTP). Web sites can present static or dynamic content. A Web site can be either internal to an organization (an intranet) or they can present information to the public over the Internet. An external Web site also may be an electronic commerce (e-commerce) portal, through which the organization may provide services over the Internet (not necessarily financial, for example the CF recruiting internet site). A Web site may be used internally within an organization to provide information, such as corporate policies, human resources forms, or a phone directory to its employees.

41. Virtually all DND/CF WANs include web sites for both informational and transactional purposes. While the intranet (DWAN) has the greatest importance to individuals within the organization, the DND/CF Internet site provides the organization's face to the public and is crucial from a public affairs perspective.

42. The following table provides recommended restoral priorities and MADs for some of the unclassified wide area networks within DND/CF:

Priority for Restoral	**Category of System**	**Information System**	**Maximum Allowable Downtime (MAD)**
1	B	Defence Wide Area Network – connectivity for Priority Users (VVIPs, Ops Centres, Regional Commanders, etc.)	2 hrs
2	A	CF Weather and Oceanographic Network Service (CFWOS) user support	4 hrs
3	B	Outlook e-mail (i.e. server outage)	4 hrs

4	B	Blackberry (e-mail) user support	4 hrs
5	B	DIN websites	24 hrs
6	B	DND/CF Internet website	24 hrs
7	B	Defence Research Establishment Network (DRENet)	24 hrs
8	B	Canadian Forces Experimental Network (CFXNet)	24 hrs
9	B	General Purpose Network (GPNet)	48 hrs
10	B	TACLANE Administration Services	48 hrs
11	B	DWAN Internet Firewall Services	48 hrs
12	B	Defence Wide Area Network (DWAN) Backbone	7 days
13	B	Non-Public Property Network (NPPNet)	7 days

ENTERPRISE (AND OTHER) APPLICATIONS

43. Enterprise applications within DND/CF typically reside on the mainframe computer located at the data centre in Borden. A mainframe is a multi-user computer designed to meet the computing needs of a large organization. The term was created to describe the large central computers developed in the late 1950s and 1960s to process bulk accounting and Information Management functions. Mainframe systems store all data in a central location rather than dispersing data among multiple machines. As a result, mainframe availability and data backups are critical.

44. Enterprise applications are in general dependent on several internal factors, including:

a. Understanding of key critical business the enterprise applications are supporting;
b. Local facilities emergency recovery;
c. Alternate data center delivery; and
d. Defence Wide Area Network (DWAN) functionality and access.

45. The single greatest enterprise application dependency is the DWAN. All enterprise applications and most other applications supporting critical systems are accessed via the DWAN. A regular assessment of threat to the DWAN is produced by CDI. These threats represent possible disruptions to the delivery of critical services. This DWAN threat assessment contains a comprehensive list of all known threats to the DWAN and ranks the likelihood of their occurrence from very low to very high. As a minimum, high value systems, which reside on and are accessed via the DWAN, will

inherit these threats. The current DWAN threat assessment document needs to be considered when assessing the likelihood of service disruption. MADs identified below are valid assuming that the bearer system, the DWAN backbone, is functional. Given that DWAN backbone outages are likely to involve much greater complexity, and a confirmed reliance on outside service providers, the MAD for the DWAN backbone may be much greater than for restoral of a single application. In fact, in many cases applications are replicated on hot standby servers, which can greatly facilitate their restoral and reduce the MAD. Thus the reason that the MAD for an application in many cases is significantly less than the MAD for the backbone on which it is dependent.

Priority for Restoral	**Category of System**	**Information System**	**Maximum Allowable Downtime (MAD)**
1	B	Canadian Forces Supply System (CFSS)	48 hrs
2	B	Central Computerized Pay System (CCPS)	72 hrs
3	B	Human Resource Management System (HRMS) 7.5 & 8.9	72 hrs
4	B	Financial Managerial Accounting System (FMAS)	72 hrs
5	B	Material Acquisition and Support Information System (MASIS) Army Navy Air Force	 48 hrs 60 hrs TBD
6	B	DIN Websites	48 hrs
7	B	DND/CF Internet website	48 hrs
8	B	Revised Pay System for Reservists (RPSR)	72 hrs
9	B	Defence Integrated Human Resources System (DIHRS) and Canadian Forces Reserve Information Management System (CFRIMS)	72 hrs
10	A	Canadian Forces Tasking Plans and Operations (CFTPO)	72 hrs
11	A	Security and Military Police Information System (SAMPIS)	72 hrs
12	A	Flight Safety Information System (FSIS)	5 days
13	C	Record Document Information Management System (RDIMS)	7 days
14	C	Court Martial Reporting System (CMRS)	7 days

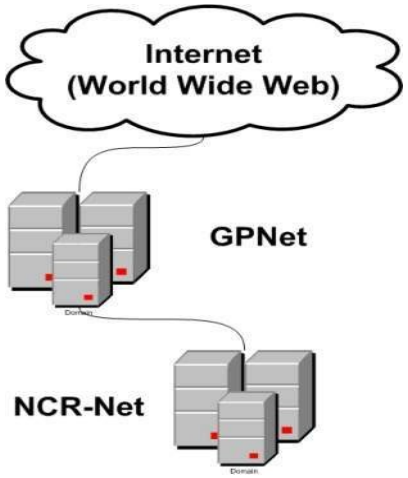
15	C	Summary Trial Database	7 days
16	B	Monitor MASS	7 days
17	B	Claims X	14 days

DESKTOP COMPUTERS AND PORTABLE SYSTEMS

46. Desktop computers are stationary personal computers (PCs) that fit conveniently on top of an office desk or table. They are not well suited to move or travel. Most desktops are networked to allow for communications with other networked devices, applications, and the Internet. Portable systems, such as laptops (also called notebook computers) or handheld computers, are PCs that can be carried for convenience and travel purposes. Portable systems are compact desktop computers that can have comparable processing, memory, and disk storage to desktop computers or limited processing memory and disk storage, such as a handheld computer. Portable systems can connect with other networked devices, applications, and the Internet through various mechanisms, such as dialup lines.

47. PCs are ubiquitous throughout the organization's IT infrastructures. Because the desktop and portable computers are the most common platform for routine automated processes, they are important elements in any contingency plan. PCs can be physically connected to an organization's LAN, can dial into the organization's network from a remote location, or can act as a stand-alone system.

48. Examples within DND/CF of PCs connected to LANs are those that collectively form the DWAN (Defence Wide Area Network – the Designated administrative network), those connected within the NCR to the NCRNet forming part of the GPNet (the unclassified network providing greater access to the Internet than DWAN), and those connected to the various classified networks (Consolidated Secret Network Infrastructure - CSNI being the most common of these). As an example of LAN/WAN topology, the following is a diagram of how the NCRNet connects users to the Internet:



49. The most common portable PC system within DND/CF is provided through DVPNI (Defence Virtual Private Network Infrastructure). DVPNI provides DND/CF

personnel who are working away from their traditional workstations with a virtual private network (VPN). Using broadband/cable and dial-up, this VPN allows remote and secure access to the Department's Protected "A" Designated administrative network, the DWAN. Should a disruptive event occur that prevents personnel access to their primary workplace, and if an alternate facility is not available, the use of DVPNI for remote access from anywhere that broadband or a telephone line (for the slower dial-up access) can provide access to the DWAN and most of the services and applications delivered through that network. BCP Coordinators having identified remote access as a contingency methodology for delivery of some critical services should ensure individuals identified to deliver those services have been equipped with and trained on the use of DVPNI terminals. Familiarity with use of the remote access system is key to continued service delivery during a crisis.

50. Capacity limitations in the number of personnel in each organization that will have access to DVPNI during a crisis situation must be factored into each organization's continuity plan – not everyone in an organization will be in a position to operate remotely based on the current footprint. As of summer 2009, the DVPNI capacity is limited to 20,000 simultaneous users remotely accessing the DWAN via high speed broadband internet access. The capacity to accommodate dial-in users is significantly less however the number of DVPNI users accessing via dial-in is quite small. More significant, though, is that only approximately 12,000 laptops have the necessary software installed and have been registered for DVPNI access, with an unknown percentage of those laptops being inactive.

51. In the event of a human resources disruptive incident (i.e. communicable disease or transit interruptions), remote access to the DWAN is only a viable continuity strategy if the means are already in place to permit such access. As the uptake on DVPNI laptops across DND/CF has been somewhat limited, this is an indicator that a more mobile and efficient means of remotely accessing the DWAN is required. ADM(IM) in conjunction with ADM(S&T) is to investigate potential technologies to permit simplified, less resource intense technologies to permit remote access to the DWAN.

52. In addition to DVPNI, certain Commanders (i.e. CDS, Comd CEFCOM, etc.) have been equipped with portable systems allowing remote connection to various classified networks (i.e. CSNI and SVCN). These HSD (High Speed Data) kits are generally provided with the ability to connect either through a broadband system or via their own integrated satellite communications capability, but in either case all data transmitted is protected with certified and accredited encryption systems.

53. Stand-alone PCs are found less commonly in the organization but often exist as a means of processing caveated (ie. Canadian Eyes Only - CEO) or classified information in locations where access to a classified LAN/WAN are not available.

54. Based on the assumption that the network backbone on which the equipment is reliant for connectivity is fully functional, the recommended priorities for restoral and MAD for desktop and portable systems (equipment) follows:

Priority for Restoral	Category of System	Information System	Maximum Allowable Downtime (MAD)
1	A/B	Desktop support to Priority Users (VVIPs, Ops Centres, Regional Commanders, etc.) (both CSNI and DWAN)	1 hr
2	A	Desktop support to users of 'small' classified systems such as SPARTAN or STONEGHOST	4 hrs
3	A	Deployed HSD kits	24 hrs
4	A	Desktop support in NCR to CSNI users	24 hrs
5	B	Desktop support in NCR to DWAN users	70% - 4 hrs NLT – 96 hrs
6	A	Security and Military Police Information System (SAMPIS) Mobile Data Terminals	48 hrs
7	C	Desktop support to GPNet users	48 hrs
8	B	DVPNI DWAN Remote Access (as this may require the user to physically bring the remote terminal to the support team, the MAD could be longer)	48 hrs
9	B	Stand-Alone PCs	3 days

IM/IT CONTINGENCY PLANNING CONSIDERATIONS SUMMARY

55. Organizations require a suite of plans to prepare themselves for response, continuity, recovery, and resumption of business processes and IT systems in the event of a disruption. As each information system within DND/CF is unique, and has different vulnerabilities and interdependencies, there are few simple, straightforward technical contingency solutions to ensure continued functioning of the system without interruption.

56. Organizations relying on information systems as an element of their Business Resumption Planning to continue delivering critical services must take into consideration that MADs as identified in this Annex generally represent a best case scenario, in which a single system fails and support staff can dedicate efforts to its restoral. In the event of a truly catastrophic disruption, it's highly feasible that multiple information systems will be affected, either through loss of utilities (i.e. electrical power) or physical damage to the systems themselves or the facility in which they are housed (i.e. fire or flood). Alternate methods of delivering service, such as manual

workarounds, must be identified and practiced to ensure that the loss of information systems does not become the sole obstacle to continued availability of critical services.